

Issues in Homeland Security Policy for the 113th Congress

William L. Painter
Analyst in Emergency Management and Homeland Security Policy

September 23, 2013

Congressional Research Service
7-5700
www.crs.gov
R42985

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

With the 10th anniversary of the establishment of the Department of Homeland Security (DHS), many observers have made a fresh assessment of where America's homeland security enterprise stands today. DHS is currently the third-largest department in the federal government, although it does not incorporate all of the homeland security functions at the federal level. The definition of homeland security remains unsettled, and questions about the effectiveness and efficiency of the department have been raised since it was first proposed. Evolution of America's response to terrorist threats has continued under the leadership of different Administrations, Congresses, and in a shifting environment of public opinion.

This report outlines an array of homeland security issues that may come before the 113th Congress. After a brief discussion of the overall homeland security budget, the report divides the specific issues into five broad categories:

- Counterterrorism and Security Management,
- Border Security and Trade,
- Immigration,
- Disaster Preparedness, Response, and Recovery, and
- Departmental Management.

Each of those areas contains a survey of topics briefly analyzed by Congressional Research Service experts. The information included only scratches the surface on most of these issues. More detailed information can be obtained by consulting the CRS reports referenced herein, or by contacting the relevant CRS expert.

Contents

What Is Homeland Security? 1
- Homeland Security: Definitions and Security 2
- The Budget and Security 3
 - DHS Appropriations 4

Counterterrorism and Security Management 5
- The Transnational Trend of Terrorism 5
- Homegrown Jihadist Terrorism 7
- Cybersecurity 10
 - Cyber Threats 11
 - Legislative Branch Efforts to Address Cyber Threats 13
 - Executive Branch Actions to Address Cyber Threats 13
- Medical Countermeasures to Chemical, Biological, Radiological, and Nuclear Terrorism 14
- BioWatch: Detection of Aerosol Release of Biological Agents 15
- Continuity of Government Operations 17
- Federal Facility Security: Federal Protective Service 18
- Food Defense 19
- Security of Pipelines 20
- Security of Chemical Facilities 22
- Security of Wastewater and Water Utilities 24

Transit Security 25

Border Security and Trade 28
- Southwest Border Issues 28
 - Spillover Violence 28
 - Illicit Proceeds and the Southwest Border 30
 - Cross-Border Smuggling Tunnels 31
- Cargo Security 32
 - Customs-Trade Partnership Against Terrorism (C-TPAT) 33
 - 100% Scanning Requirement 34
 - Port of Entry (POE) Infrastructure and Personnel 36
- Domestic Nuclear Detection 37
- Transportation Worker Identification Credential (TWIC) 38
- Aviation Security 40
 - Explosives Screening Strategy for the Aviation Domain 40
 - Risk-Based Passenger Screening 42
 - The Use of Terrorist Watchlists in the Aviation Domain 43
 - Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft 44
 - Security Issues Regarding the Operation of Unmanned Aircraft 45

Immigration 47
- Immigration Inspections at Ports of Entry 47
- Entry-Exit System 49
- Enforcement Between Ports of Entry 51
- CBP Integrity 53

Disaster Preparedness, Response, and Recovery 54
- Disaster Assistance Funding 54

Hurricane Sandy Recovery 56
DHS State and Local Preparedness Grants 58
Consolidation of DHS State and Local Programs 59
Firefighter Assistance Programs 60
Emergency Communications Infrastructure and Technology 61
Presidential Policy Directive 8 and the National Preparedness System 62
Public Health and Medical Services 63
Potential Reauthorization of the Defense Production Act of 1950 64
Management Issues at DHS 66
DHS Reorganization Authority 66
The Management Budget 67
DHS Financial Management Reforms 68
Headquarters Consolidation 70
Department of Homeland Security Personnel Issues 71
Recruitment and Hiring of Highly Qualified Candidates 71
Diversity of the Workforce 73
Employee Morale 74
Acquisition 75
Acquisition Workforce 75
Balanced Workforce Strategy (BWS) 76
Homeland Security Research and Development 77

Tables

Table 1. Congressional Funding for Transit Security, FY2002-FY2012 27

Contacts

Author Contact Information 79

What Is Homeland Security?

This question has dogged U.S. public policy debates for more than a decade. There is no statutory definition of homeland security that reflects the breadth of the enterprise as currently understood. Although there is a federal Department of Homeland Security, it is neither solely dedicated to homeland security missions, nor is it the only part of the federal government with significant responsibilities in this arena.

The Department of Homeland Security (DHS) was established by the Homeland Security Act of 2002 (P.L. 107-296), which was signed into law on November 25, 2002. The new department was assembled from components pulled from 22 different government agencies and began official operations on March 1, 2003. Since then, DHS has undergone a series of restructurings and reorganizations to improve its effectiveness and efficiency.

Although DHS does include many of the homeland security functions of the federal government, several of these functions or parts of these functions remain at their original executive branch agencies and departments, including the Departments of Justice, State, Defense, and Transportation. Not all of the missions of DHS are officially "homeland security" missions. Some components have historical missions that do not directly relate to conventional homeland security definitions, such as the Coast Guard's environmental and boater safety missions, and Congress has in the past debated whether FEMA and its disaster relief and recovery missions belong in the department.

Some aspects of crime and justice could arguably be included in a broad definition of homeland security. Issues such as the role of the military in law enforcement, monitoring and policing transfers of money, human trafficking, explosives and weapons laws, and aspects of foreign policy, trade, and economics have implications for homeland security policy.

Rather than trying to resolve the question of what is and is not homeland security, this report is limited to topics that generally fall within the four mission study areas used to develop the Quadrennial Homeland Security Review mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53):

- Counterterrorism and Security Management,
- Border Security and Trade,
- Immigration, and
- Disaster Preparedness, Response, and Recovery.

A fifth section covering management issues at DHS rounds out the discussion. As each topic is introduced, the lead expert and author of the section is listed, along with their contact information. In many cases, a specific CRS report is highlighted as a source of more detailed information.

The issues included in this report do not represent a comprehensive list of possible issues—they represent a broad array of issues likely to be addressed by Congress in the coming months.

Homeland Security: Definitions and Security

Shawn Reese, Analyst in Emergency Management and Homeland Security Policy
(sreese@crs.loc.gov, 7-0635)

For more information, see CRS Report R42462, *Defining Homeland Security: Analysis and Congressional Considerations*.

Twelve years after the 9/11 terrorist attacks, policymakers continue to debate the definition of homeland security. Prior to 9/11, the United States addressed crises through the separate prisms of national defense, law enforcement, and emergency management. 9/11 prompted a strategic process that included a discussion about and the development of homeland security policy. Today, this debate and development has resulted in numerous federal entities with homeland security responsibilities. Presently, there are over 30 federal departments, agencies, and entities that have homeland security responsibilities and receive annual appropriations to execute homeland security missions.

Congress is responsible for appropriating funds for homeland security missions and priorities. These priorities need to exist and to be clear in order for funding to be most effective. Presently, homeland security is not funded based on clearly defined strategic priorities. In an ideal scenario, there would be a consensus definition of homeland security; as well as prioritized missions, goals, and activities. Policymakers could then use a process based on these defined priorities to incorporate feedback and strategically respond to new facts and situations as they develop.

The debate over and development of homeland security definitions and priorities persists as the federal government continues to issue and implement homeland security strategies. The first homeland security strategy document issued by President George W. Bush's Administration was the 2003 *National Strategy for Homeland Security*, which was revised in 2007. In 2008, the Department of Homeland Security (DHS) issued the *Strategic Plan—One Team, One Mission, Securing Our Homeland*. The 2007 *National Strategy for Homeland Security* primarily focused on terrorism, whereas the 2008 *Strategic Plan* included references to all-hazards and border security. Arguably, the 2003 and 2007 National Strategies for Homeland Security addressed terrorism due to such incidents as the 9/11 terrorist attacks and the attempted bombing of American Airlines Flight 93 on December 22, 2001, whereas the 2008 Strategic Plan addressed terrorism and all-hazards due to natural disasters such as Hurricane Katrina, which occurred in 2005. These documents have been superseded by several other documents which are now considered the principal homeland security strategies.

The White House and DHS are the principle source of homeland security strategies. The current primary national homeland security strategic document is the 2010 *National Security Strategy*, which unlike the 2007 *National Strategy for Homeland Security* addresses all hazards and is not primarily terrorism focused.[1] DHS's strategic documents are the 2010 *Quadrennial Homeland Security Review*; the 2010 *Bottom-Up Review*; and the 2012 *Strategic Plan*. DHS states that these documents are nested in the 2010 *National Security Strategy* and DHS is currently developing the 2014 *Quadrennial Homeland Security Review*.[2] At the national level, the 2010 National Security

[1] President Obama's Administration specifically addresses terrorism and counterterrorism in the 2011 *National Strategy for Counterterrorism*.

[2] DHS states that it intends to issue the 2014 Quadrennial Homeland Security Review in late 2013 or early 2014.

Strategy guides not just DHS's activities, but also all federal government homeland security activities. The development of national homeland security strategy will continue as the Obama Administration and DHS develop and implement such strategies as the 2014 *Quadrennial Homeland Security Review* and a potentially new *National Security Strategy* that the Obama Administration may issue sometime in the next four years.

It has been argued that homeland security, at its core, is about coordination because of the disparate stakeholders and risks.[3] Many observers assert that homeland security is not only about coordination of resources and actions to counter risks; it is also about the coordination of the strategic process policymakers use in determining the risks, the stakeholders and their missions, and the prioritization of those missions.

Without a general consensus on the literal and philosophical definition of homeland security, achieved through a strategic process, some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation. From this perspective, general consensus on the homeland security concept necessarily starts with a consensus definition and an accepted list of prioritized missions that are constantly reevaluated to meet risks of the homeland security paradigm of the 21st century. The varied homeland security definitions and concepts represented in the current national and homeland security strategy documents, however, may be the result of a strategic process that has attempted to, in an ad hoc manner, adjust federal homeland security policy to emerging threats and risks.

The Budget and Security

William L. Painter, Analyst in Emergency Management and Homeland Security Policy (wpainter@crs.loc.gov, 7-3335)

For more information, see CRS Report R43147, *Department of Homeland Security: FY2014 Appropriations*.

According to data from the Office of Management and Budget (OMB), the entire U.S. government spent $564 billion (in nominal dollars) on "homeland security"—defined in law as "those activities that detect, deter, protect against, and respond to terrorist attacks occurring within the United States and its territories"[4]—in the 10 years after the 9/11 attacks. Such spending peaked in FY2009 at $73.8 billion. The total budget request for homeland security activities for FY2014 was $72.7 billion, a reduction of $1.1 billion from its high-water mark in nominal terms.[5]

By comparison, the budget for the Department of Homeland Security has grown from $31.2 billion in FY2003, when it did not have its own appropriations bill, to $59.9 billion in FY2012, the last year for which we have complete budget data. Roughly $35.1 billion, or 58.6%, is considered "homeland security" spending by OMB's accounting under the above definition. Some argue that the definition in law is too focused on explicit and directly attributable

[3] Donald F. Kettl, *System Under Stress: Homeland Security and American Politics*, 2nd ed, Washington, DC, *CQPress*, 2007, p. 82.

[4] 116 Stat. 2251. The law refers to a definition from OMB's 2002 "Annual Report to Congress on Combatting Terrorism."

[5] Office of Management and Budget, *FY2014 Analytical Perspectives: Budget of the United States Government*, p.415.

counterterrorism activities compared to broader theories that have been part of the national discussion, which consider immigration and border control or disaster response as a part of homeland security.

DHS Appropriations

In 2010, neither the House nor the Senate completed work on its version of a FY2011 appropriations bill for the Department of Homeland Security. For the first time, the department, like the rest of the federal government that year, was funded through a long-term continuing resolution. This resolution established funding levels for some components and activities, while leaving others to be funded at FY2010 levels. The resolution overall gave the department much less explicit direction from Congress than previous funding vehicles, in several cases leaving decisions usually made by Congress about how to allocate limited funds in DHS's hands.[6] This stood in contrast to previous years, when at least one body passed an appropriations bill funding the department, and legislation providing specific appropriations was either passed on a stand-alone basis or as part of legislation including multiple bills. Just as importantly, in those years, either a conference report or explanatory statement of the managers provided further direction to the department on allocation of appropriated funds, oversight requirements and other expressions of congressional intent.

For both FY2012 and FY2013, DHS was funded through consolidated appropriations legislation, which carried traditional levels of specific Congressional direction for the department. The actual level of budgetary resources available for the FY2013 budget year, however, was impacted by the across-the-board cuts—known as sequestration—mandated by the Budget Control and Deficit Reduction Act of 2011 (BCA). A combination of factors has therefore made the final funding levels for FY2013 difficult to ascertain, including the fact that:

- Some activities were legislatively exempt from sequestration;
- Sequestration was implemented before the final appropriations legislation for FY2013 was enacted, so the across-the-board reduction was taken against a baseline determined by OMB, rather than the actual amount appropriated; and
- Federal agencies have been encouraged to use the budgetary flexibility afforded them—the ability to transfer funds between accounts and to reprogram funding within accounts—to protect some activities deemed more important at the expense of others.

Although an expenditure plan was submitted to Congress on April 26, 2013, which outlined the post-sequester funding levels provided to DHS in the consolidated appropriations act for FY2013[7] before the exercise of budgetary flexibility, it did not include resources provided through supplemental appropriations for disaster relief.[8] No official statement of final FY2013 post-sequester funding levels by program, project, and

[6] For a fuller discussion of this issue, see CRS Report R41189, *Homeland Security Department: FY2011 Appropriations*, coordinated by Jennifer E. Lake and William L. Painter.

[7] P.L. 113-6. Analysis of the DHS appropriation in the act can be found in CRS Report R42644, *Department of Homeland Security: FY2013 Appropriations*.

[8] P.L. 113-2. Analysis of the supplemental appropriation for FY2013 can be found in CRS Report R42869, *FY2013 Supplemental Funding for Disaster Relief*.

activity after the exercise of transfer and reprogramming authority has been made, and is not expected until the release of the FY2015 budget request.

As of this writing, the FY2014 annual appropriation for DHS is unresolved, as are the other eleven annual appropriations bills. For FY2014, the Administration's total discretionary appropriations request for DHS was $44.7 billion, including funding for disaster relief and overseas contingency operations (which do not count against the budget allocation of the bill). Comparable calculations for House-passed and Senate-reported DHS appropriations legislation show similar total funding levels, $44.6 billion and $44.7 billion, respectively. However, the appearance of general agreement on the rough funding level for the department should not be interpreted as a clear path forward for the legislation. The full Senate has not taken up its version of the bill as of this writing. There are significant differences in the policy direction and proposed funding levels that make up the bill's overall total, and the resolution of these differences and the precise funding level itself is linked to the resolution of the FY2014 budget and the other FY2014 appropriations bills.

Some sort of resolution on the size of the overall FY2014 budget will be necessary in order to complete the appropriations process, either through annual appropriations legislation, continuing resolutions, or a combination. The debate in FY2014 hinges in part on whether to continue with the automatic cuts mandated in the BCA as amended. These reductions in the overall discretionary spending cap total $91.6 billion, or roughly 8.7% of the total discretionary budget. The limit on discretionary defense spending described by current law is $497 million, and $469 million for non-defense discretionary spending.[9] Homeland security activities as defined in law are funded with both defense and non-defense budget authority, although most of the DHS budget falls in the non-defense category.

The current budget environment will likely present challenges to homeland security programs and the department going forward, as ongoing capital investment efforts and staffing needs will compete with the budget demands of the rest of the government for limited funds. The potential impact of the changed budget environment is discussed at various points throughout this report.

Counterterrorism and Security Management

The Transnational Trend of Terrorism

John Rollins, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529)

For more information, see CRS Report R41004, *Terrorism and Transnational Crime: Foreign Policy Issues for Congress*.

Terrorism remains a transnational threat that entails risks to U.S. global interests emanating from and manifested in both the international and domestic environment. Central to U.S. efforts to address transnational terrorism are actions taken to detect, deter, and defeat Al Qaeda. While recognizing that numerous other terrorist groups may wish to harm U.S. global security interests, the Administration primarily focuses on addressing threats from Al Qaeda, its affiliated

[9] CBO, *Final Sequestration Report for Fiscal Year 2013*, March 2013, p. 4.

organizations, and adherents to its violence-based philosophy. Speaking before the United Nations Counterterrorism Committee, Daniel Benjamin, the Coordinator of the Office of the Counterterrorism at the State Department, said "Rather than trying to combat directly every single terrorist organization regardless of whether they have the intent or capability to ever attack the U.S. or our citizens, President Obama's counterterrorism strategy is (focused on) Al Qaeda and its affiliates and adherents."[10] Understanding how Al Qaeda continues to evolve into a global entity with a diverse set of actors and capabilities is central to formulating sound strategic policy and overseeing its effective implementation.

The past few years have witnessed an increase in terrorist actions by entities claiming some affiliation with or philosophical connection to Al Qaeda. Many of the past year's global terrorist attacks were conducted by individuals or small terrorist cells that received support ranging from resources and training to having minimal connections, if any, with the terrorist groups to which they claim allegiance. Some argue that recent U.S. counterterrorism successes may be reducing the level of terrorist threats to the nation emanating from core Al Qaeda. U.S. officials suggest that the killing of Osama bin Laden in May 2011 coupled with continuous post-9/11 global military and intelligence counterterrorism actions have significantly degraded Al Qaeda's ability to successfully launch a catastrophic terrorist attack against U.S. global interests. Others suggest that Al Qaeda has changed from an organization to a philosophical movement, making it more difficult to detect and defeat. These security experts suggest that Al Qaeda and associated affiliates will remain viable, due in part to the prospective security implications related to the nation's budgetary situation. Noted author on counterterrorism issues Daveed Gartenstein-Ross argues that "The U.S. will not be (defeated) by Al Qaeda. But one can see that as the national debt increases, we (will) have to make spending cuts and as Al Qaeda gets stronger in multiple countries simultaneously—Somalia, Yemen, Pakistan, maybe Mali—suddenly you're looking at multiple theaters from where catastrophic strikes can be launched."[11] In August 2013 the Director of the Federal Bureau of Investigation noted concerns associated with Al Qaeda inspired entities also migrating to the countries of Tunisia, Libya, Algeria, Egypt, and Syria.[12]

The balance between ensuring effective counterterrorism policies and being mindful of the current budget environment is not lost on senior Administration officials. In recent years John Brennan, in his former capacity as the Assistant to the President for Homeland Security, now the Director of the Central Intelligence Agency, has spoken of Osama bin Laden's often stated objective of pursuing global acts of terrorism against the nation's interests with the desire to "bleed [the U.S.] financially by drawing us into long, costly wars that also inflame anti-American sentiment."[13]

The terrorist threat to U.S. global interests will likely remain an important issue for the Administration and remainder of the 113th Congress. Over the past few years numerous individuals were arrested in the homeland and abroad for conducting attacks and planning

[10] Remarks by Daniel Benjamin, Coordinator, State Department, Office of the Coordinator for Counterterrorism, Before the United Nations Counterterrorism Committees, July 20, 2011.

[11] Spencer Ackerman, "Even Dead, Osama Has a Winning Strategy," *Wired*, July 20, 2011, http://www.wired.com/dangerroom/2011/07/even-dead-osama-has-a-winning-strategy-hint-its-muhammad-alis/.

[12] Pierre Thomas, Jack Cloherty, and Mike Levine, "Outgoing FBI Director Warns of Americans Traveling to Syria and Bringing Terrorist Tactics Home," ABC News, Aug. 22, 2013, Outgoing FBI Director Warns of Americans Traveling to Syria and Bringing Terrorist Tactics Home.

[13] Remarks by the John Brennan, the Assistant to the President for Homeland Security and Counterterrorism, before the Paul H. Nitze School of Advanced International Studies, June 29, 2011.

terrorism-related activities directed at U.S. national security interests. All of the attacks—successful and unsuccessful—were of a transnational dimension and ranged from a lone shooter who appears to have become radicalized over the Internet to terrorist organizations wishing to use airliners as platforms for destruction to individuals attempting to detonate large quantities of explosives in symbolic areas frequented by large groups of people.

Thus far the 113th Congress undertook efforts, largely through hearings, to better understand the nature of terrorism in various geographic regions and assess the effectiveness of U.S. and partnering nations' counterterrorism efforts. Programs and policies that the 113th Congress have reviewed include public diplomacy efforts; imposition of sanctions; terrorism financing rules; the nexus between international crime, narcotics, and terrorism; and the relationship between domestic and international terrorism activities. The 113th Congress may continue to assess the Obama Administration's counterterrorism-related strategies, policies, and programs to ascertain if additional guidance or legislation is required. These assessments will likely entail considerations of how best to balance perceived risks to U.S. global security interests with concerns about the long-term fiscal challenges facing the nation.

Homegrown Jihadist Terrorism[14]

Jerome P. Bjelopera, Specialist in Organized Crime and Terrorism (jbjelopera@crs.loc.gov, 7-0622)

For more information, see CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*.

CRS estimates that, since May 2009, arrests have been made in 50 homegrown jihadist[15] terrorist plots by American citizens or legal permanent residents of the United States as part of a much-discussed apparent uptick in terrorist activity in the United States.[16] Three of these plots resulted in attacks—the bombing of the 2013 Boston Marathon allegedly committed by Tamerlan and Dzhokhar Tsarnaev; U.S. Army Major Nidal Hasan's assault at Fort Hood in Texas; and Abdulhakim Muhammed's shooting at the U.S. Army-Navy Career Center in Little Rock, AR—that produced 17 deaths.[17] By comparison, in more than seven years from the September 11, 2001, terrorist strikes (9/11) through May 2009, there were 21 such plots.[18] Two resulted in attacks, and never more than six occurred in a single year (2006).[19] The apparent spike in such

[14] CRS does not presume the guilt of indicted individuals in pending federal cases.

[15] For this report, "homegrown" describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. "Jihadist" describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and adhere to the model of the immediate followers and companions of the Prophet Muhammad.

[16] In a January 13, 2013, report, CRS listed 63 plots and attacks by homegrown jihadists that occurred between September 11, 2001, and December 2012. The number has risen since then, as additional plots occurred after December 2012. See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera. Hereinafter: Bjelopera, *American Jihadist*.

[17] In addition, the Tsarnaevs also allegedly killed a police officer after the Boston Marathon bombing.

[18] For more information on these attacks see Appendix A in Bjelopera, *American Jihadist.*

[19] The two attacks between 9/11 and May 2009 involved Hasan Akbar and Mohammed Reza Taheri-Azar. On March (continued...)

activity after May 2009 suggests that at least some Americans—even if a tiny minority—are susceptible to ideologies supporting a violent form of jihad. Most of the homegrown plots after May 2009 likely reflect a trend in jihadist terrorist activity away from schemes directed by core members of significant terrorist groups such as Al Qaeda.

The Threat: Four Key Themes

Homegrown violent jihadist activity since 9/11 defies easy categorization. CRS analysis of the terrorist plots and attacks since 9/11 suggests four broad themes:

- **Various Endgames:** Plots have involved individuals interested in a variety of ways to harm U.S. interests. Some individuals focused on becoming foreign fighters in conflict zones, such as Somalia. Others planned attacks using explosives, incendiary devices, or firearms. Yet others incorporated multiple, unspecific, or unique tactics. Finally, outside of the post-9/11 violent plots, additional individuals intended only to fund or materially support jihadist activities.
- **Little Interest in Martyrdom:** A minority of homegrown jihadists clearly exhibited interest in killing themselves while engaged in violent jihad.
- **Success of Lone Wolves:** Individuals acting alone, so-called "lone wolves," conducted all four successful homegrown attacks since 9/11.
- **Divergent Capabilities:** The operational capabilities of participants diverge greatly. Some evinced terrorist tradecraft such as bomb-making skills. Others appeared to be far less experienced.

Countering the Threat

The Obama Administration has acknowledged the significance of the homegrown jihadist threat in two of its recent strategy documents. In June 2011 it announced its *National Strategy for Counterterrorism*.[20] The strategy focuses on Al Qaeda, its affiliates (groups aligned with it), and its adherents (individuals linked to or inspired by the terrorist group).[21] John Brennan, at the time President Obama's top counterterrorism advisor, publicly described the strategy as the first one "that designates the homeland as a primary area of emphasis in our counterterrorism efforts."[22]

(...continued)

23, 2003, two days after the U.S. invasion of Iraq, U.S. Army Sergeant Akbar killed two U.S. Army officers and wounded 14 others at U.S. Army Camp Pennsylvania in Kuwait, 25 miles from the Iraq border. On March 3, 2006, Taheri-Azar, a 22-year-old naturalized American citizen from Iran, drove his sport utility vehicle (SUV) into a crowd at The Pit, a popular student gathering spot at the University of North Carolina at Chapel Hill. The SUV struck and injured several people.

[20] White House, *National Strategy for Counterterrorism,* June 2011, http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf. Hereinafter: *National Strategy.*

[21] Ibid, p. 3.

[22] Mathieu Rabechault, "U.S. Refocuses on Home-Grown Terror Threat," *AFP,* June 29, 2011; Karen DeYoung, "Brennan: Counterterrorism Strategy Focused on al-Qaeda's Threat to Homeland," *Washington Post*, June 29, 2011.

In 2011, the Obama Administration also released a strategy for combating violent extremism.[23] It revolves around countering the radicalization of all types of potential terrorists. As such, the radicalization of violent jihadists falls under its purview. The strategy's domestic focus includes philosophical statements about the importance of protecting civil rights, federal cooperation with local leaders in the private and public sectors, and the insistence that the strategy does not center solely on fighting one particular radical ideology.[24]

Radicalization

Radicalization has been described as the exposure of individuals to ideological messages and the movement of those individuals from mainstream beliefs to extremist viewpoints.[25] Others define it more simply, as changes in belief and behavior to justify intergroup violence and personal or group sacrifice to forward specific closely held ideas.[26] The United Kingdom's "Prevent" counter-radicalization strategy defines radicalization as "the process by which a person comes to support terrorism and forms of extremism leading to terrorism."[27] The Obama Administration's counter-radicalization strategy frames its discussion around "violent extremists," which it defines as "individuals who support or commit ideologically-motivated violence to further political goals."[28]

While the concept of "radicalization" and its possible end result of "terrorism" are certainly related, an important distinction between the terms exists as they relate to the threshold of U.S. law enforcement interest and action. This is because Americans have the right under the First Amendment to adopt, express, or disseminate ideas, even hateful and radical ones. But when radicalized individuals mobilize their views (i.e., move from a radicalized viewpoint to membership in a terrorist group, or to planning, materially supporting, or executing terrorist activity), then the nation's public safety and security interests are activated.

In the post-9/11 environment, the public expects law enforcement to disrupt terrorist plots *before* an attack occurs. This has led authorities to adopt a preventive policing approach that focuses not just on crime that has occurred, but on the possibility that a crime may be committed in the future. In this context, a major challenge for federal law enforcement, particularly the Federal Bureau of Investigation (FBI), is gauging how quickly and at what point individuals move from radicalized beliefs to violence so that a terrorist plot can be detected and disrupted. A 2008 revision to the *Attorney General's Guidelines for Domestic Federal Bureau of Investigation Operations* was intended to be helpful in this regard, streamlining FBI investigations and making them more proactive. The revision permits the bureau to conduct assessments of individuals or groups without factual predication.[29] However, the new guidelines have generated some controversy.

[23] White House, *Empowering Local Partners to prevent Violent Extremism in the United States,* August 2011, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

[24] For more information on the strategy, see CRS Report R42553, *Countering Violent Extremism in the United States*, by Jerome P. Bjelopera. Eileen Sullivan, "New White House Strategy to Hit Violent Extremism," *Associated Press,* August 3, 2011.

[25] Royal Canadian Mounted Police, National Security Criminal Investigations, *Radicalization: A Guide for the Perplexed*, Canada, June 2009, p. 1.

[26] Clark McCauley and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," *Terrorism and Political Violence*, vol. 20, no. 3 (July 2008), p. 416.

[27] Home Office, *Prevent Strategy,* June 2011, p. 108, http://www.homeoffice.gov.uk/publications/counter-terrorism/prevent/prevent-strategy/prevent-strategy-review?view=Binary.

[28] *Empowering Local Partners to Prevent Violent Extremism in the United States,* August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

[29] According to the FBI, "Although difficult to define, 'no particular factual predication' is less than 'information or allegation' as required for the initiation of a preliminary investigation (PI). For example, an assessment may be (continued...)

Civil libertarians have questioned their impacts on privacy.[30] Also, the bombing of the 2013 Boston Marathon has prompted some to ask whether the FBI appropriately shared information with state and local officials regarding an assessment of Tamerlan Tsarnaev its agents conducted in 2011.[31]

To counter violent jihadist plots, U.S. and foreign law enforcement have employed two sets of innovative tactics. Using violations of civil laws to arrest and prosecute suspected terrorists and their support networks is known as taking the "Al Capone" approach, in reference to the federal government's successful use of the mobster's violations of tax law to incarcerate him. Law enforcement has also successfully used "agents provocateurs"—people employed to associate with suspects and incite them to commit acts that they can be arrested for. These tactics have long been used in a wide variety of criminal cases but have particular utility in counterterrorism investigations as they allow suspects to be arrested prior to the commission of a terrorist act rather than after the damage has been done.

Cybersecurity

John Rollins, Specialist in Terrorism and National Security (jrollins@crs.loc.gov, 7-5529)

For more information, see CRS Report R40836, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*.

Cyber threats to the United States are a current and growing concern to policymakers. Technology is ubiquitous and relied upon in almost every facet of modern life, such as supporting government services, corporate business processes, and individual professional and personal pursuits. Many of these technologies are interdependent and the disruption to one piece of equipment may have a negative cascading effect on other devices. A denial of service, theft or manipulation of data, or damage to critical infrastructure through a cyber-based attack could have significant impacts on national security, the economy, and the livelihood of individual citizens. These concerns raise many questions for Congress, among them,

- Who are the aggressors in cyberspace and what are their intentions and capabilities?
- What are the impacts and implications of cyberattacks?
- What legislative and policy actions have the Congress and executive branch taken to respond to threats from cyberspace? What further steps should be taken?

(...continued)

conducted when: (i) there is reason to collect information or facts to determine whether there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. An FBI employee must be able to explain the authorized purpose and the clearly defined objective(s), and reason the particular investigative methods were used to conduct the Assessment." See Federal Bureau of Investigation, *Domestic Investigations and Operations Guide*, redacted, 2011 update, pp. 5–1 through 5–2.For more information see CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

[30] Charlie Savage, "F.B.I. Agents Get Leeway to Push Privacy Bounds," *New York Times,* June 12, 2011.

[31] Scott Shane and Michael S. Schmidt, "Boston Police Weren't Told F.B.I. Got Warning on Brother," *New York Times,* May 9, 2013. FBI press release, "Statement by Special Agent in Charge Richard DesLauriers Regarding Information Sharing," May 9, 2013.

Cyber Threats

Cyber-based technologies[32] are now ubiquitous around the globe. The vast majority of their users pursue lawful professional and personal objectives. However, criminals, terrorists, and spies also rely heavily on cyber-based technologies to support organizational objectives. These malefactors may access cyber-based technologies in order to deny service, steal or manipulate data, or use a device to launch an attack. Entities using cyber-based technologies for illegal purposes take many forms and pursue a variety of actions counter to U.S. global security and economic interests.

The threats posed by these cyber-aggressors and the examples of types of attacks they can pursue are not mutually exclusive. For example, a hacker targeting the intellectual property of a corporation may be categorized as both a cyberthief and a cyberspy. A cyberterrorist and cyberwarrior may be employing different technological capabilities in support of a nation's security and political objectives. Commonly recognized cyber-aggressors and representative examples of the harm they can inflict include the following:

Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks as a form of terrorism. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, and a means of communication.[33] While no unclassified reports have been published regarding a cyberattack on a critical component of the nation's infrastructure, the vulnerability of critical life-sustaining control systems being accessed and destroyed via the Internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed.[34]

Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. For example, a 2011 FBI report noted, "a company was the victim of an intrusion and had lost 10 years' worth of research and development data—valued at $1 billion—virtually overnight."[35] Likewise, in 2008 the Department of Defense's (DOD's) classified computer network system was unlawfully accessed and "the computer code, placed there by a foreign intelligence agency, uploaded itself undetected onto both classified and unclassified systems from which data could be transferred to servers under foreign control."[36] Reportedly, the intelligence community will soon complete a classified National Intelligence Estimate focused on

[32] Defined as an electronic device that accesses or relies on the transfer of bytes of data to perform a mechanical function. The device can access cyberspace (Internet) through the use of physical connections or wireless signals.

[33] For additional information, see CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

[34] See "Challenges Remain in DHS' Efforts to Security Control Systems," Department of Homeland Security, Office of Inspector General, August 2009. For a discussion of how computer code may have caused the halting of operations at an Iranian nuclear facility see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[35] Executive Assistant Director Shawn Henry, *Responding to the Cyber Threat*, Federal Bureau of Investigation, Baltimore, MD, 2011.

[36] Department of Defense Deputy Secretary of Defense William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, October 2010.

cyberspying against U.S. targets from abroad. Many cybersecurity experts expect this report to address activities relating to the "Chinese government's broad policy of encouraging theft of intellectual property through cyberattacks."[37] Then-DOD Secretary Leon Panetta reportedly stated, "it's no secret that Russia and China have advanced cyber capabilities."[38]

Cyberthieves are individuals who engage in illegal cyber-attacks for monetary gain.[39] Examples include an organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a financial account. One estimate has placed the annual cost of cybercrime to individuals in 24 countries at $388 billion.[40] However, given the complex and sometimes ambiguous nature of the costs associated with cybercrime, and the reluctance in many cases of victims to admit to being attacked, there does not appear to be any publicly available, comprehensive, reliable assessment of the overall costs of cyberattacks.

Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives.[41] These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyberattack and are often blamed by the host country when accusations are levied by the nation that has been attacked. Often, when a foreign government is provided evidence that a cyberattack is emanating from its country, the nation that has been attacked is informed that the perpetrators acted of their own volition and not at the behest of the government. In August 2012 a series of cyberattacks were directed against Saudi Aramco, the world's largest oil and gas producer and most valuable company, according to the *New York Times*. The attacks compromised 30,000 of the company's computers and the code was apparently designed to disrupt or halt the production of oil. Some security officials have suggested that Iran may have supported this attack. However, numerous cyberwarrior groups, some with linkages to nations with objectives counter to those of Saudi Arabia, have claimed credit for this incident.[42]

Cyberactivists are individuals who perform cyberattacks for pleasure, philosophical, or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist" such as a member of a group who undertakes an attack for political reasons. The activities of these groups can range from simple nuisance-related denial of service attacks to disrupting government and private corporation business processes.

[37] Ken Dilanian, "U.S. Spy Agencies to Detail Cyberattacks from Abroad," *Los Angeles Times*, December 6, 2012.

[38] Ibid.

[39] For discussions of federal law and issues relating to cybercrime, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, and CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[40] Symantec, "Symantec Internet Security Threat Report: Trends for 2010," Vol. 16, April 2011. Plain text summary with calculations available at http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

[41] For additional information, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[42] Perlroth, Nicole, "Cyberattack On Saudi Firm Disquiets U.S.," *New York Times*, October 24, 2012, p. A1. Available at http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

Ascertaining information about the aggressor and their capabilities and intentions is very difficult.[43] The threats posed by these aggressors coupled with the United States' proclivity to be an early adopter of emerging technologies,[44] which are often interdependent and contain vulnerabilities, make for a complex environment when considering operational responses, policies, and legislation designed to safeguard the nation's strategic economic and security interests.

Legislative Branch Efforts to Address Cyber Threats[45]

More than 50 federal statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place. While revisions to most of those laws have been proposed over the past few years, no major cybersecurity legislation has been enacted since 2002. Recent legislative proposals, including many bills introduced in the 111th and 112th Congresses, have focused largely on issues in 10 broad areas: national strategy and the role of government, reform of the Federal Information Security Management Act (FISMA), protection of critical infrastructure (including the electricity grid and the chemical industry), information sharing and cross-sector coordination, breaches resulting in theft or exposure of personal data such as financial information, cybercrime, privacy in the context of electronic commerce, international efforts, research and development, and the cybersecurity workforce.

For most of those topics, at least some of the bills addressing them have proposed changes to current laws. Several of the bills specifically focused on cybersecurity received committee or floor action, but none became law prior to the 113th Congress. Many observers believe that enactment of cybersecurity legislation will be attempted again in the 113th Congress.

Executive Branch Actions to Address Cyber Threats[46]

In 2008, the George W. Bush Administration established the Comprehensive National Cybersecurity Initiative (CNCI) through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Those documents are classified, but the Obama Administration released a description of them in March 2010.[47] Goals of the 12 initiatives in that description include consolidating external access points to federal systems; deploying

[43] The concept of *attribution* in the cyber world entails an attempt to identify with some degree of specificity and confidence the geographic location, identity, capabilities, and intention of the cyber-aggressor. Mobile technologies and sophisticated data routing processes and techniques often make attribution difficult for U.S. intelligence and law enforcement communities.

[44] Emerging cyber-based technologies that may be vulnerable to the actions of a cyber-aggressor include items that are in use but not yet widely adopted or are currently being developed. For additional information on how the convergence of inexpensive, highly sophisticated, and easily accessible technology is providing opportunities for cyber-aggressors to exploit vulnerabilities found in a technologically laden society see *Global Trends 2030: Alternative Worlds, National Intelligence Council, Office of the Director of National Intelligence, December 10, 2012*.

[45] Information derived from a multi-authored CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer, November 9, 2012.

[46] Information contained in this section was derived from a multi-authored reports and memos produced by numerous CRS analysts working on cybersecurity.

[47] The White House, "The Comprehensive National Cybersecurity Initiative," March 5, 2010. For additional information about this Initiative and associated policy considerations, see CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John W. Rollins and Anna C. Henning.

intrusion detection and prevention systems across those systems; improving research coordination and prioritization and developing "next-generation" technology, information sharing, and cybersecurity education and awareness; mitigating risks from the global supply chain for information technology; and clarifying the federal role in protecting critical infrastructure.

In December 2009, the Obama Administration created the position of White House Cybersecurity Coordinator. The responsibilities for this position include government-wide coordination of cybersecurity-related issues, including overseeing the implementation of the CNCI. The Coordinator works with both the National Security and Economic Councils in the White House. However, the Coordinator does not have direct control over agency budgets, and some observers argue that operational entities such as the DOD's National Security Agency (NSA) have far greater influence over federal cybersecurity issues.[48] Reportedly, in October 2012 President Obama signed a classified Presidential Decision Directive that "enables the military to act more aggressively to thwart cyberattacks on the Nation's web of government and private computer networks."[49]

The complex federal role in cybersecurity involves both securing federal systems, assisting in protecting nonfederal systems, and pursuing military, intelligence, and law enforcement community detection, surveillance, defensive, and offensive initiatives. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems and dozens of agencies have government-wide aggressor, issue, and critical infrastructure sector-specific responsibilities and legislative authorities. The cybersecurity roles and responsibilities of these agencies are often complementary but at times are overlapping or competing. In the absence of enactment of cybersecurity legislation, the White House issued an executive order on February 12, 2013, "directing federal departments and agencies to use their existing authorities to provide better cybersecurity for the Nation."[50]

Medical Countermeasures to Chemical, Biological, Radiological, and Nuclear Terrorism

Frank Gottron, Specialist, Science and Technology Policy (fgottron@crs.loc.gov, 7-5854)

The anthrax attacks of 2001 highlighted the nation's vulnerability to biological terrorism. The federal government responded to these attacks by increasing efforts to protect civilians against chemical, biological, radiological, and nuclear (CBRN) terrorism. Successful deployment of effective medical countermeasures, such as drugs or vaccines, could reduce the effects of a CBRN attack. The federal government has created several programs over the last decade to develop, procure, and distribute CBRN medical countermeasures. Despite these efforts, the pharmaceutical industry has developed few new countermeasures, and many experts question the government's ability to quickly distribute countermeasures following an attack. The 113th

[48] See, for example, Seymour M. Hersh, "Judging the Cyber War Terrorist Threat," *The New Yorker*, November 1, 2010.

[49] Nakashima, Ellen, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *The Washington Post*, Nov. 14, 2012.

[50] Daniel, Michael, "Improving the Security of the Nation's Critical Infrastructure," The White House Blog, February 13, 2013. http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure.

Congress will likely consider the effectiveness of the federal efforts and whether these programs should be continued, modified, or ended.

In 2004, Congress passed the Project BioShield Act (P.L. 108-276) to encourage the private sector to develop CBRN medical countermeasures by creating a guaranteed federal market.[51] Congress advance appropriated $5.6 billion for Project BioShield acquisitions for FY2004-FY2013. Through August 2013, the federal government had obligated $2.8 billion of this advance appropriation to acquire CBRN countermeasures. Additionally, Congress removed $2.3 billion from this account through rescission or transfers to other programs. The 113th Congress passed the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013 (PAHPRA, P.L. 113-5) that authorized $2.8 billion in advance funding for Project BioShield through FY2018. The 113th Congress may still consider whether modifying the funding amount or providing appropriations on an annual basis would improve the program's efficiency or performance.

In light of the current fiscal environment, Congress is likely to increase its scrutiny of the planning, coordination, and accountability of federal efforts to research, develop, and procure CBRN medical countermeasures. To this end, PAHPRA requires additional planning and transparency by requiring detailed annual countermeasure strategy and implementation plans and a coordinated multi-year budget. Congress may also consider nontraditional programs that may improve the efficiency of existing efforts, such as the President's request to create a nonprofit, nongovernmental strategic investment corporation to provide capital and business advice to small companies developing medical countermeasure-related technologies.[52]

Distribution of existing medical countermeasures during a CBRN emergency remains a challenge for the federal government and its partners. The federal government maintains programs that stockpile and distribute stores of medical countermeasures, including the Centers for Disease Control and Prevention's Strategic National Stockpile (SNS). Many experts question the sufficiency of these federal programs, and whether state governments have sufficient plans, organization, and resources to receive and effectively disseminate federal stockpiles.[53] Congress is likely to continue evaluating the effectiveness of federal programs and may also consider whether to augment these efforts with other stockpiling and distribution methods. Such methods include stockpiling countermeasures at homes or businesses and using the U.S. Postal Service to distribute countermeasures. These proposals may raise some concerns regarding program costs, unintended use of countermeasures, and local implementation.

BioWatch: Detection of Aerosol Release of Biological Agents

Sarah A. Lister, Specialist in Public Health and Epidemiology (slister@crs.loc.gov, 7-7320)

[51] CRS Report R42349, *The Project BioShield Act: Issues for the 112th Congress*, by Frank Gottron.

[52] U.S. Department of Health and Human Services, *Public Health and Social Services Emergency Fund Justification of Estimates for Appropriations Committees FY2013*, p. 18.

[53] See, for examples, Senator Bob Graham, Senator James Talent, and Randall Larsen, et al., *Bio-Response Report Card*, The Bipartisan WMD Terrorism Research Center, Washington, DC, October 2011, pp. 45-49, http://www.wmdcenter.org/wp-content/uploads/2011/10/bio-response-report-card-2011.pdf; and Christopher Nelson, Andrew M. Parker, and Shoshana R. Shelton, et al., *Analysis of the Cities Readiness Initiative* (Santa Monica, CA: RAND Corporation, 2012), pp. 31-34.

The BioWatch program—launched in 2003—deploys sensors in more than 30 large U.S. cities to detect the possible aerosol release of a bioterrorism pathogen, in order that medications can be distributed to the population before exposed individuals become ill. Air filters in the sensors are collected daily and tested for biological agents. The DHS Office of Health Affairs (OHA) is responsible for system management, including operational costs and procurements. The Under Secretary for Science and Technology advises the Secretary regarding research and development efforts and priorities in general, in support of the department's missions. The Centers for Disease Control and Prevention (CDC) in the Department of Health and Human Services (HHS) is responsible for some aspects of BioWatch laboratory testing. Local jurisdictions are responsible for the public health response to a bioterrorism incident. BioWatch has not detected such an incident since its inception, although it has detected pathogens of interest; scientists believe that natural airborne "background" levels of these pathogens may exist in certain regions.

In July 2012, the *Los Angeles Times* published the first in a series of investigative articles criticizing the performance of the current BioWatch system.[54] The articles claimed that the system is prone to "false alarms" and is also insufficiently sensitive to detect an actual incident. The DHS Assistant Secretary for Health Affairs published a response disputing these claims.[55] In addition, some state and local health officials defended the program, saying, among other things, that it has fostered collaboration among federal, state, and local officials, who would be called upon to work together in response to an actual incident.[56]

Because prompt treatment may minimize casualties in a bioterrorism event, federal officials have sought to reduce the inherent delay in daily BioWatch filter collection by developing so-called autonomous sensors. These sensors would analyze filter deposits and transmit results in near-real time. OHA has been pursuing procurement of this type of sensor, which it terms Generation 3, or Gen-3, since 2007. However, according to the Government Accountability Office (GAO), "BioWatch Gen-3 has a history of technical and management challenges."[57] In particular, "Gen-3's estimated life cycle cost, some $5.8 billion, makes it one of the largest DHS acquisitions. And the question is, whether it justifies that level of investment."[58] GAO recommended that before continuing the acquisition, "DHS reevaluate the mission need and alternatives and develop performance, schedule, and cost information in accordance with guidance and good acquisition

[54] David Willman, "The Biodefender That Cries Wolf," *Los Angeles Times*, July 8, 2012.

[55] Dr. Alexander Garza, Assistant Secretary for Health Affairs, DHS, "The Truth About BioWatch: The Importance of Early Detection of a Potential Biological Attack," July 12, 2012. Statistics cited in this blog posting were later reported to be inaccurate by a DHS official. See comments of BioWatch Program Manager Dr. Mike Walter before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Continuing Concerns Over BioWatch and the Surveillance of Bioterrorism*, 113th Cong., 1st sess., June 18, 2013, CQ transcription.

[56] See for example Robert Roos, "Public Health Officials Respond to Critique of BioWatch," *CIDRAP News*, August 17, 2012, http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/news/aug1712biowatch.html.

[57] GAO, *Biosurveillance: DHS Should Reevaluate Mission Need and Alternatives before Proceeding with BioWatch Generation-3 Acquisition*, GAO-12-810, September 10, 2012, p. 3, http://www.gao.gov/products/GAO-12-810.

[58] Testimony of William Jenkins, Director, Homeland Security and Justice Issues, GAO, before the House Homeland Security Committee, Subcommittee on Emergency Preparedness, Response and Communications, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, *BioWatch Present and Future: Meeting Mission Needs for Effective Biosurveillance?*, joint hearing, 112th Cong., 2nd sess., September 13, 2012, CQ transcription. According to GAO, the estimated Gen-3 life cycle costs are based on DHS's June 2011 Life-Cycle Cost Estimate, which estimates costs through FY2028.

practices."[59] In June 2013, DHS announced that it had paused Gen-3 deployment to conduct an analysis of alternatives in response to GAO's recommendation.[60]

The performance of the BioWatch program has attracted the attention of Members of Congress since the program's inception. Congressional appropriators have at times sought to limit funding for program expansion and/or called for program reviews.[61] Authorizing committees in each Congress since the 108th have held hearings on the program. In the 112th Congress, the House Committee on Energy and Commerce began an investigation of the program, which it has continued in the 113th Congress.[62] In August 2013, committee leadership asked GAO for a new study of the technical capabilities of the Gen-3 system intended for deployment.[63]

Continuity of Government Operations

R. Eric Petersen, Specialist in American National Government, Government and Finance Division (epetersen@crs.loc.gov, 7-0643)

Continuity of government operations refers to programs and initiatives to ensure that governing entities are able to recover from a wide range of potential operational interruptions. Government continuity planning may be viewed as a process that incorporates preparedness capacities, including agency response plans, employee training, recovery plans, and the resumption of normal operations. These activities are established in part to ensure the maintenance of civil authority, provision of support for those affected by an incident, infrastructure repair, and other actions in support of recovery. Arguably, any emergency response presumes the existence of an ongoing, functional government to fund, support, and oversee recovery efforts. Interruptions for which contingency plans might be activated include localized acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents.

Current authority for executive branch continuity programs is provided in a 2007 National Security Presidential Directive (NSPD) 51 on National Continuity Policy.[64] To support the provision of essential government activities, NSPD 51 sets out a policy "to maintain a comprehensive and effective continuity capability composed of continuity of operations[65] and

[59] GAO, *Biosurveillance: DHS Should Reevaluate Mission Need and Alternatives before Proceeding with BioWatch Generation-3 Acquisition*, GAO-12-810, September 10, 2012, highlights page.

[60] Testimony of BioWatch Program Manager Dr. Mike Walter before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Continuing Concerns over BioWatch and the Surveillance of Bioterrorism*, 113th Cong., 1st sess., June 18, 2013.

[61] See BioWatch discussions in CRS Reports on annual DHS appropriations, http://www.crs.gov/pages/subissue.aspx?cliid=2345.

[62] House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, "Oversight and Investigations Subcommittee Continues Investigation of BioWatch and Surveillance of Bioterrorism," press release, June 18, 2013, with links to committee report and other documents, http://energycommerce.house.gov/press-releases.

[63] House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, "Bipartisan Committee Leadership Requests GAO Study of BioWatch," press release, Aug. 20, 2013, http://energycommerce.house.gov/press-releases.

[64] White House, Office of the Press Secretary, *National Security and Homeland Security Presidential Directive*, May 9, 2007, HSPD 51 is also identified as Homeland Security Presidential Directive (HSPD) 20 A more detailed discussion of national continuity policy is available in CRS Report RS22674, *National Continuity Policy: A Brief Overview*, by R. Eric Petersen.

[65] NSPD 51 identifies continuity of operations (COOP) as "an effort within individual executive departments and (continued...)

continuity of government[66] programs in order to ensure the preservation of our form of government[67] under the Constitution and the continuing performance of national essential functions (NEF) under all conditions."

Executive Order (E.O.) 12656, Assignment of Emergency Preparedness Responsibilities, was issued in 1988,[68] and assigns national security emergency preparedness responsibilities to federal executive departments and agencies. E.O. 12656 requires the head of each federal department and agency to "ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities." Subsequent sections require each department to carry out specific contingency planning activities in its areas of policy responsibility.

Although contingency planning authorities are chiefly based on presidential directives, Congress could consider whether current authorities accurately reflect current government organization and goals, the costs of these programs, potential conflicts that might result from departments and agencies complying with different authorities, and the extent to which government contingency planning ensures that the federal executive branch will be able to carry out its responsibilities under challenging circumstances.

Federal Facility Security: Federal Protective Service

Shawn Reese, Analyst in Emergency Management and Homeland Security Policy (sreese@crs.loc.gov, 7-0635)

For more information, see CRS Report R41138, *Federal Building, Courthouse, and Facility Security*.

The federal government's real property[69] is comprised over 900,000 assets.[70] The security of this federal property affects not only the daily operations of the federal government but the safety of federal employees and the public. A number of these properties are multi-tenant federal buildings that house federal courthouses, and some congressional state and district offices. Security of federal facilities includes physical security assets such as closed-circuit television cameras, barrier material, and security personnel.

(...continued)

agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies."

[66] NSPD 51 identifies continuity of government (COG) as "a coordinated effort within the federal government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency."

[67] The directive notes "that each branch of the federal government is responsible for its own continuity programs," and requires an executive branch official to "ensure that the executive branch's COOP and COG policies ... are appropriately coordinated with those of the legislative and judicial branches in order to … maintain a functioning federal government." The legislative branch and the federal judiciary maintain continuity programs consonant with their positions as coequal branches of government. NSPD 51 does not specify the nature of appropriate coordination with continuity planners in the legislative and judicial branch.

[68] 53 FR 47491; November 23, 1988.

[69] Real property is defined as property that is leased or owned by the General Services Administration.

[70] U.S. Government Accountability Office, Federal Real Property: Overreliance on Leasing Contributed to High-Risk Designation, GAO-11-879T, August 4, 2011, p. 1, http://www.gao.gov/new.items/d11879t.pdf.

The Federal Protective Service (FPS) is designated as the lead "Government Facilities Sector Agency" for the National Infrastructure Protection Plan, and as such is responsible for the protection and security of federally owned and leased buildings, property, and personnel. In general, FPS undertakes security and law enforcement activities that reduce vulnerability to criminal and terrorist threats, which include all-hazards based risk assessments; emplacement of criminal and terrorist countermeasures, such as vehicle barriers and closed-circuit video cameras; law enforcement response; assistance to federal agencies through facility security committees; and emergency and safety education programs. FPS also assists other federal agencies, such as the U.S. Secret Service at National Special Security Events. FPS employs approximately 1,225 law enforcement officers, investigators, and administrative personnel; and it administers the services of approximately 15,000 contract security guards.[71] Federal agencies protected by FPS pay fees that are established by the Office of Management and Budget. FPS's funding is derived from those fees.

Federal facility security practices have been subject to criticism by government auditors and security experts, and have been the topic of congressional oversight hearings. Elements that have received criticism include the use of private security guards, FPS management and security practices, and the coordination of federal facility security. According to FPS, it plans to (1) improve the strategic methods used in identifying and reducing actual and potential threats directed at FPS-protected facilities; (2) restore proactive monitoring activities to mitigate the increased risk to these facilities; (3) improve the service provided by contract security guard forces through acquisition strategies and "intensive" monitoring and training; (4) develop risk-based security standards tied to intelligence and risk-assessments; (5) refine business practices through stakeholder interface; and (6) implement a capital plan that will improve security and customer service.[72] Congress will likely continue oversight of FPS management and operations in the 113th Congress to ensure that it has the necessary staffing, resources, and funding to carry out its mission.

Food Defense

Sarah A. Lister, Specialist in Public Health and Epidemiology (slister@crs.loc.gov, 7-7320)

Foods may be intentionally contaminated for purposes of terrorism, fraud (e.g., the dilution of a valuable commodity), or other harmful intent. Food safety efforts have long focused on protecting against unintentional contaminants, such as infectious pathogens or pesticide residues. Since the 2001 terrorist attacks, regulators and others have added a focus on *food defense*, the protection of the food supply from deliberate or intentional acts of contamination or tampering.[73] Large-scale foodborne outbreaks can sicken hundreds of people. Sales of affected commodities—as well as unaffected commodities that the consuming public perceives to be involved—can suffer. An intentional incident of food contamination, especially if it were an act of terrorism, could have serious economic consequences, in addition to any illnesses it caused.

[71] U.S. Department of Homeland Security, National Protection and Programs Directorate, *Federal Protective Service: Fiscal Year 2012 Congressional Justification*, Washington, DC, February 2011, p. FPS-1.

[72] U.S. Department of Homeland Security, National Protection and Programs Directorate, *Federal Protective Service: Strategic Plan, Secure Facilities, Safe Occupants*, Washington, DC, 2011, pp. 3-5.

[73] Food and Drug Administration (FDA), "Food Defense," http://www.fda.gov/Food/FoodDefense.

Federal food safety responsibility rests primarily with the U.S. Department of Agriculture (USDA) and the Food and Drug Administration (FDA). USDA's Food Safety and Inspection Service (FSIS) regulates most meat and poultry and some egg products; FDA is responsible for the safety of most other foods.[74] State and local authorities assist with inspection, outbreak response, and other food safety functions, and regulate retail establishments. Noting the complexity of the nation's food and agriculture sector, which accounts for about one-fifth of the nation's economy, DHS says that "FDA is responsible for the safety of 80 percent of the food consumed in the United States ... FDA regulates $240 billion of domestic food and $15 billion of imported food. In addition, roughly 600,000 restaurants and institutional food service providers, an estimated 235,000 grocery stores, and other food outlets are regulated by State and local authorities that receive guidance and other technical assistance from FDA."[75]

The 111th Congress enacted a comprehensive food safety law, the Food Safety Modernization Act (FSMA, P.L. 111-353), focused mainly on foods regulated by FDA.[76] FSMA attempts to prevent both intentional and unintentional contamination of foods through a variety of strategies to prevent food contamination and through enhanced regulatory authorities. However, FDA has not yet implemented some of the law's provisions.[77] In addition, FSMA requires the Secretaries of Health and Human Services and Agriculture to develop a National Agriculture and Food Defense Strategy, implementation plan, and research agenda. This strategy and the accompanying documents have not yet been published.[78]

GAO has named food safety as a high-risk issue, citing the fragmentation of federal oversight, among other concerns.[79] GAO specifically noted delays in the implementation of the nation's food and agriculture defense policy, Homeland Security Presidential Directive 9 (HSPD-9). This directive, issued by the George W. Bush Administration in 2004, assigns various emergency response and recovery responsibilities to USDA, FDA, DHS, and other agencies. GAO found that there is no centralized coordination of HSPD-9 implementation efforts, and recommended that DHS take on this role to assure that the nation's food and agriculture defense policy is fully in place. In addition, GAO recommended that the executive branch develop a government-wide performance plan for all of its food safety activities.

Security of Pipelines

Paul Parfomak, Specialist in Energy and Infrastructure Policy, Resources, Science and Industry Division (pparfomak@crs.loc.gov, 7-0030)

For more information, see CRS Report R41536, *Keeping America's Pipelines Safe and Secure: Key Issues for Congress*.

[74] CRS Report RS22600, *The Federal Food Safety System: A Primer*, by Renée Johnson.

[75] DHS, *National Infrastructure Protection Plan: Agriculture and Food Sector Snapshot*, http://www.dhs.gov/food-and-agriculture-sector.

[76] CRS Report R40443, *The FDA Food Safety Modernization Act (P.L. 111-353)*, coordinated by Renée Johnson.

[77] FDA FSMA implementation information, http://www.fda.gov/Food/GuidanceRegulation/FSMA/default.htm.

[78] FDA, FSMA Reports and Studies, http://www.fda.gov/Food/GuidanceRegulation/FSMA/ucm271961.htm.

[79] GAO, "Revamping Federal Oversight of Food Safety," http://www.gao.gov/highrisk/revamping_food_safety/.

Nearly a half-million miles of high-volume pipeline transport natural gas, oil, and other hazardous liquids across the United States.[80] These pipelines are integral to U.S. energy supply and link to other critical infrastructure, such as power plants, airports, and military bases. While a fundamentally safe means of transport, gas and oil pipelines, globally, have been a favored target of terrorists, militants, and organized crime. Since September 11, 2001, U.S. officials have foiled plots to attack jet fuel pipelines at the John F. Kennedy International Airport and to attack the Trans Alaska Pipeline System and a major natural gas pipeline in the eastern United States.[81] Although Al Qaeda attacks on U.S. pipelines are perceived as unlikely, attacks by individuals unaffiliated with organized or terrorist groups may be a growing concern. For example, in August 2011, federal agents arrested a U.S. citizen—acting alone—who confessed to planting an explosive device under a natural gas pipeline in Oklahoma.[82] In June 2012, a man was critically injured attempting to plant an explosive device along a natural gas pipeline in Plano, TX.[83] One specific area of pipeline security that has recently come to the fore is cybersecurity. In March 2012, the Industrial Control Systems Cyber Emergency Response Team within DHS identified an ongoing series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011 "positively identified … as related to a single campaign."[84]

Federal pipeline security activities are led by the Pipeline Security Division within the Transportation Security Administration (TSA). Although the TSA has statutory authority to regulate pipeline security, to date, these activities have relied upon voluntary industry compliance with federal security guidance and TSA security best practices. TSA has been engaged in a number of specific pipeline security initiatives since 2003, including developing security standards; implementing measures to mitigate security risk; building and maintaining stakeholder relations, coordination, education, and outreach; and monitoring compliance with voluntary pipeline security standards. The cornerstone of TSA's pipeline activities is its Corporate Security Review (CSR) program, wherein the agency visits the largest pipeline and natural gas distribution operators to review their security plans and inspect their facilities. TSA has completed CSRs covering the largest 100 pipeline systems (84% of total U.S. energy pipeline throughput) and is in the process of conducting second CSRs of these systems.[85] In 2008, the TSA initiated its Critical Facility Inspection Program (CFI) to conduct in-depth inspections of all the critical facilities of the 125 largest pipeline systems in the United States. TSA concluded the CFI program in May 2011, having completed a total of 347 facility inspections throughout the United States.[86]

While TSA is generally credited with significantly strengthening U.S. pipeline security, Congress has had ongoing concerns about the adequacy of the agency's pipeline security standards, its

[80] Hazardous liquids primarily include crude oil, gasoline, jet fuel, diesel fuel, home heating oil, propane, and butane. Other hazardous liquids transported by pipeline include anhydrous ammonia, carbon dioxide, kerosene, liquefied ethylene, and some petrochemical feedstocks.

[81] U.S. Attorney's Office, Middle District of Pennsylvania, "Man Convicted of Attempting to Provide Material Support to Al-Qaeda Sentenced to 30 Years' Imprisonment," Press release, November 6, 2007; U.S. Dept. of Justice, "Four Individuals Charged in Plot to Bomb John F. Kennedy International Airport," Press release, June 2, 2007.

[82] Carol Cratty, "Man Accused in Attempted Bombing of Oklahoma Gas Pipeline," CNN, August 12, 2011.

[83] "Grand Jury Indicts Plano Gas Pipeline Bomb Suspect on Weapons Charge," *Associated Press*, July 11, 2012.

[84] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Gas Pipeline Cyber Intrusion Campaign," *ICS-CERT Monthly Monitor*, April 2012, p.1, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

[85] Government Accountability Office (GAO), *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867, August, 2010, Executive Summary.

[86] Transportation Security Administration, personal communication with section author, February 24, 2012.

overall level of resources, and certain aspects of its CSR program. Because the TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well.[87] But some Members of Congress, as well as the Department of Transportation's Office of Inspector General, have questioned the adequacy of voluntary, rather than mandatory, federal pipeline security requirements.[88] In 2010, a Member expressed concern that TSA's pipeline division—with 13 full-time equivalent staff—did not have sufficient staff to carry out a federal pipeline security program on a national scale.[89] In a 2010 report, the Government Accountability Office recommended a number of specific actions to improve TSA's pipeline security priority-setting and CSR assessment processes, such as transmitting CSR recommendations in writing to pipeline operators.[90] To date, there has been no federal legislation directly addressing these concerns, but they may receive additional attention in the 113th Congress. In addition to these specific issues, the next Congress may assess how pipeline security fits together with the U.S. pipeline safety program, administered by the DOT, in the nation's overall strategy to protect transportation infrastructure. While the DOT and TSA have distinct missions, pipeline safety and security are intertwined.

Security of Chemical Facilities

Dana A. Shea, Specialist in Science and Technology Policy (dshea@crs.loc.gov, 7-6844)

For more information, see CRS Report R42918, *Chemical Facility Security: Issues and Options for the 113th Congress* and CRS Report R43070, *Regulation of Fertilizers: Ammonium Nitrate and Anhydrous Ammonia*.

Congress provided DHS authority to regulate security at chemical facilities in the Homeland Security Appropriations Act, 2007 (P.L. 109-295, §550). This authority expires on October 4, 2013. Congressional policymakers are considering a range of actions in the 113th Congress, including an extension or revision of this authority. Even before the explosion of the West Fertilizer Company in West, TX, various stakeholders had criticized the content of DHS regulation and the effectiveness and pace of its implementation and recommended changes to the underlying statute. Recommended statutory changes include broadening the regulated community,[91] enabling the federal government to require adoption of particular security measures at facilities,[92] and increasing access to currently confidential vulnerability information. Other

[87] Jack Fox, General Manager, Pipeline Security Division, Transportation Security Administration (TSA), remarks before the Louisiana Gas Association Pipeline Safety Conference, New Orleans, LA, July 25, 2012.

[88] U.S. Dept. of Transportation, Office of Inspector General*, Actions Needed to Enhance Pipeline Security, Pipeline and Hazardous Materials Safety Administration*, Report No. AV-2008-053, May 21, 2008, p. 6.

[89] The Honorable Gus M. Billirakis, Remarks before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight hearing on "Unclogging Pipeline Security: Are the Lines of Responsibility Clear?," Plant City, FL, April 19, 2010.

[90] U.S. Government Accountability Office, *Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes*, GAO-10-867 August 4, 2010, pp. 56-57.

[91] See, for example, Testimony of Rand Beers, Under Secretary, National Protection and Programs Directorate, Department of Homeland Security, before the Senate Committee on Homeland Security and Governmental Affairs, March 3, 2010.

[92] See, for example, Testimony by Paul Orum, Blue Green Chemical Security Coalition/ Independent Consultant to Center for American Progress, before the House Committee on Energy and Commerce, Subcommittee on Environment (continued...)

stakeholders, including many industry representatives, support an extension of the existing authority without any changes.[93]

DHS regulates chemical facilities for security purposes. The Obama Administration and other stakeholders have determined that existing regulatory exemptions, such as for community water systems and wastewater treatment facilities, pose potential risks. Environmental and "right-to-know" groups additionally advocate that Congress include requirements for facilities to adopt or identify "inherently safer technologies" and widely disseminate security-related information to first responders and employees. The regulated industry generally opposes granting DHS the ability to require implementation of inherently safer technologies or other specific security measures. They question the maturity and applicability of the inherently safer technology concept as a security measure and cite the need to tailor security approaches for each facility. The Obama Administration has identified potential security concerns if chemical security-related information is more broadly disseminated, but the discovery that information about the chemical inventory of the West Fertilizer Company was not effectively shared between federal agencies has led to reconsideration of existing information sharing policies. The Obama Administration issued Executive Order 13650, Improving Chemical Facility Safety and Security, to begin a multiagency effort to coordinate federal efforts. Challenges facing policymakers include whether to extend or change the existing statutory authority, whether to mandate consideration or implementation of inherently safer technologies, what the appropriate balance is between protecting security information and releasing information to non-governmental stakeholders, and how to assess and potentially ameliorate costs associated with implementing required security measures.

While the DHS regulatory program is still in its early stages, it has experienced significant implementation challenges and delays. Few of the thousands of regulated chemical facilities have fully complied with the DHS chemical security regulations,[94] the Government Accountability Office estimates that it will be seven to nine years before DHS has completed review and approval of information submitted by regulated facilities,[95] and congressional policymakers have questioned the efficacy of DHS regulatory activities.[96] Policymakers performing oversight of the program face critical decisions regarding program changes. Significant changes could increase implementation delays, but such changes may be most effective if made early in the program's implementation, rather than later after companies have invested in specific security measures.

(...continued)

and the Economy, September 11, 2012.

[93] See, for example, Testimony of Matthew J. Leary, Pilot Chemical Company, on behalf of the Society of Chemical Manufacturers and Affiliates, before the House Committee on Energy and Commerce, Subcommittee on Environment and the Economy, September 11, 2012.

[94] Testimony of David Wulf, Director, Infrastructure Security Compliance Division, National Programs and Protection Directorate, Department of Homeland Security, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, on August 1, 2013.

[95] Government Accountability Office, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353, April 2013.

[96] See, for example, Representative Robert Aderholt, Chairman, Subcommittee on Homeland Security, House Committee on Appropriations, Opening Statement as Prepared for Delivery at Hearing on Chemical Security Anti-Terrorism Standards Program, July 26, 2012.

Security of Wastewater and Water Utilities

Claudia Copeland, Specialist in Resources and Environmental Policy,
(ccopeland@crs.loc.gov, 7-7227)

For more information, see CRS Report RL32189, *Terrorism and Security Issues Facing the Water Infrastructure Sector.*

The systems that comprise the nation's water supply and water quality infrastructure have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Across the country, these systems consist of 16,000 publicly owned wastewater treatment facilities and 168,000 public drinking water facilities, plus thousands of miles of pipes, aqueducts, water distribution, and sewer lines. Damage or destruction could disrupt the delivery of vital human services, threatening public health and the environment, or possibly causing loss of life. In recognition, Congress and other policymakers have considered a number of initiatives in this area, including enhanced physical security of water infrastructure facilities, improved communication and coordination, and research. Recent policy interest has focused on two issues: (1) security of wastewater utilities, and (2) whether to include wastewater and water utilities in chemical plant security regulations implemented by DHS.

When Congress created DHS in 2002,[97] it gave DHS responsibility to coordinate information to secure the nation's critical infrastructure, including the water sector, through partnerships with the public and private sectors. Under Homeland Security Presidential Directive 7, the Environmental Protection Agency (EPA) is the lead federal agency for protecting wastewater and drinking water utility systems, because EPA has regulatory authority over both types of water utilities under the Clean Water Act and the Safe Drinking Water Act, respectively. Separately, in P.L. 107-188,[98] Congress required drinking water systems serving more than 3,300 persons to conduct vulnerability analyses and to submit the assessments to EPA. Congressional committees have on several occasions considered legislation to encourage or require wastewater treatment facilities to similarly conduct vulnerability assessments and develop site security plans (such as H.R. 2883 in the 111th Congress), but no bill has been enacted.

Congress also has been considering requirements for wastewater and drinking water utilities in connection with legislation to establish risk-based and performance-based security standards at the nation's chemical plants (see discussion of "Security of Chemical Facilities"). Issues debated for some time include (1) whether to preserve an existing exemption for water utilities from chemical facility standards or include them in the scope of DHS rules under the Chemical Facility Anti-Terrorism Standards program (CFATS); and (2) whether water utilities that store or use extremely hazardous substances, such as chlorine gas, should be required to consider the use of different chemicals or safer processes (so-called "inherently safer technology"). A third issue is what roles EPA and DHS should play in implementing such requirements and generally in overseeing homeland security at wastewater and drinking water utilities. There has been considerable debate about coordination between EPA and DHS and whether EPA's lead role for the water utility sector should be altered. Water utilities have urged Congress not to create a dual or split regulatory arrangement between two agencies, arguing that EPA has long-standing

[97] P.L. 107-297; 116 Stat. 2322.

[98] The Public Health Security and Bioterrorism Preparedness and Response Act, 116 Stat. 594.

expertise in wastewater and water regulatory and security issues. Others have argued that DHS should have overall responsibility.

Legislative proposals addressing these issues that received committee approval in the 112th Congress differed in a number of respects but reflected apparent consensus regarding water utility issues: they would have preserved the existing exemption from the DHS CFATS program, and none would have mandated inherently safer technology. Further, none would have altered EPA's lead role for the water utility sector. None of these bills was enacted by the 112th Congress. A provision of the Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6), extended authority for the existing CFATS program through October 4, 2013. In addition, legislation that would extend statutory authority for the CFATS program for another year, through October 4, 2014 (H.R. 2217), has passed the House and been reported by the Senate Appropriations Committee.[99]

Other legislation introduced in the 113th Congress (S. 67, the Secure Water Facilities Act) would add coverage of wastewater and drinking water facilities in the CFATS program and would require certain facilities in the water sector that handle chemicals to take action to reduce the consequences of a terrorist attack, such as using different chemicals, or changing to inherently safer technology (IST). The bill would not alter EPA's lead role in regulating wastewater facilities and community water systems for security purposes.

Since the terrorist attacks of 2001, wastewater and water utilities have been engaged in numerous activities to assess potential vulnerabilities and strengthen facility and system protections. Congressional oversight of this sector's homeland security activities has been limited but could be of interest in the 113th Congress.

Transit Security

David Randall Peterman, Analyst in Transportation Policy (dpeterman@crs.loc.gov, 7-3267)

For more information, see CRS Report RL33512, *Transportation Security: Issues for the 113th Congress*.

Bombings of passenger trains in Europe and Asia in the past several years illustrate the vulnerability of passenger rail systems to terrorist attacks. Passenger rail systems—primarily subway systems—in the United States carry about five times as many passengers each day as do airlines, over many thousands of miles of track, serving stations that are designed primarily for easy access. The increased security efforts around air travel have led to concerns that terrorists may turn their attention to "softer" targets, such as transit or passenger rail. A key challenge Congress faces is balancing the desire for increased rail passenger security with the efficient functioning of transit systems, with the potential costs and damages of an attack, and with other federal priorities.

[99] The CFATS anti-terrorism standards were mandated in DHS funding legislation enacted in 2006 (P.L. 109-295). They were initially established on an interim basis for three years, but Congress has been extending them on a year-to-year basis.

The volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening airline passengers undergo. Consequently, transit security measures tend to emphasize managing the consequences of an attack. Nevertheless, steps have been taken to try to reduce the risks, as well as the consequences, of an attack. These include vulnerability assessments; emergency planning; emergency response training and drilling of transit personnel (ideally in coordination with police, fire, and emergency medical personnel); increasing the number of transit security personnel; installing video surveillance equipment in vehicles and stations; and conducting random inspections of bags, platforms, and trains.

The challenges of securing rail passengers are dwarfed by the challenge of securing bus passengers. There are some 76,000 buses carrying 19 million passengers each weekday in the United States. Some transit systems have installed video cameras on their buses, and Congress has provided grants for security improvements to intercity buses. But the number and operation characteristics of transit buses make them all but impossible to secure.

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), passed by Congress on July 27, 2007, included provisions on passenger rail and transit security and authorized $3.5 billion for FY2008-FY2011 for grants for public transportation security. The act required public transportation agencies and railroads considered to be high-risk targets by DHS to have security plans approved by DHS (§§1405 and 1512). Other provisions required DHS to conduct a name-based security background check and an immigration status check on all public transportation and railroad frontline employees (§§1414 and 1522), and gave DHS the authority to regulate rail and transit employee security training standards (§§1408 and 1517).

In 2010 TSA completed a national threat assessment for transit and passenger rail, and in 2011 completed an updated transportation systems-sector specific plan, which established goals and objectives for a secure transportation system. The three primary objectives for reducing risk in transit are to:

- mitigate risks to high-risk/high-consequence assets;
- expand operational deterrence activities; and
- enhance information sharing.[100]

TSA surface transportation security inspectors conduct assessments of transit systems (and other surface modes) through the agency's Baseline Assessment for Security Enhancement (BASE) program. The agency has also developed a security training and security exercise program for transit (I-STEP), and its Visible Intermodal Prevention and Response (VIPR) teams conduct operations with local law enforcement officials, including periodic patrols of transit and passenger rail systems, to create "unpredictable visual deterrents."

The House Committee on Homeland Security's Subcommittee on Transportation Security held a hearing in May 2012 to examine the surface transportation security inspector program. As discussed at the hearing, the number of inspectors had increased from 175 in FY2008 to 404 in FY2011 (full-time equivalents). Issues considered at the hearing included the lack of surface transportation expertise among the inspectors, many of whom were promoted from screening passengers at airports; the administrative challenge of having the surface inspectors managed by

[100] Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2013 Congressional [Budget] Justification*, p. 14.

federal security directors who are located at airports, and who themselves typically have no surface transportation experience; and the security value of the tasks performed by surface inspectors.[101]

The Department of Homeland Security (DHS) provides grants for security improvements for public transit, passenger rail, and occasionally other surface transportation modes under the Urban Area Security Initiative program (see **Table 1**). The vast majority of the funding goes to public transit providers. The Transit Security Grant Program (TSGP) did not receive a specified amount of funding in FY2012, as Congress left program funding allocations to the discretion of DHS.

Table 1. Congressional Funding for Transit Security, FY2002-FY2012

Fiscal year	Appropriation (millions of dollars)
2002	$63[a]
2003	65
2004	50
2005	108
2006	131
2007	251
2008	356
2009	498[b]
2010	253
2011	200
2012	88[c]
2013	84
Total	$2,063

Source: FY2002: Department of Defense FY2002 Appropriations Act, P.L. 107-117; FY2003: FY2003 Emergency Wartime Supplemental Appropriations Act, P.L. 108-11; FY2004: Department of Homeland Security FY2004 Appropriations Act, P.L. 108-90; FY2005-FY2011: United States Government Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, GAO-12-303, February 2012, Table 1; FY2012: DHS, *Transit Security Grant Program FY2012 Funding Opportunity Announcement*; FY2013: DHS, *FY2013 Transit Security Grant Program FY2013 Funding Opportunity Announcement*

Notes: The Transit Security Grant Program was formally established in FY2005; in FY2003-FY2004, grants were made through the Urban Areas Security Initiative. Does not include funding provided for security grants for intercity passenger rail (Amtrak), intercity bus service, and commercial trucking.

a. Appropriated to Washington Metropolitan Area Transit Authority and the Federal Transit Administration.

b. Includes $150 million provided in the American Recovery and Reinvestment Act.

c. Congress did not specify an amount for transit security grants, leaving funding to the discretion of DHS.

[101] United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, Hearing on *TSA's Surface Inspection Program: Strengthening Security or Squandering Resources?*, May 31, 2012, http://homeland.house.gov/hearing/subcommittee-hearing-tsa%E2%80%99s-surface-inspection-program-strengthening-security-or-squandering.

In a February 2012 report, the Government Accountability Office found opportunity for duplication among four DHS state and local security grant programs with similar goals, one of which was the public transportation security grant program.[102] The Obama Administration proposed consolidating several of these programs in the FY2013 budget. This proposal was not supported by congressional appropriators, though appropriators have expressed concerns that grant programs have not focused on areas of highest risk and that significant amounts of previously appropriated funds have not yet been awarded to recipients.[103]

Border Security and Trade

Southwest Border Issues

Spillover Violence

Kristin M. Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

For more information, see CRS Report R41075, *Southwest Border Violence: Issues in Identifying and Measuring Spillover Violence*.

There has been an elevated level of drug trafficking-related violence within and between the drug trafficking organizations (DTOs) in Mexico, and some estimates have placed the number of drug trafficking-related deaths in Mexico between December 2006 (when Mexican President Felipe Calderón began his campaign against the DTOs) and December 2012 (when the Calderón administration ended) at somewhere between 45,000 and 55,000.[104] Mexican DTOs have been at war with each other as well as with the Mexican police and military personnel who are attempting to enforce the drug laws in northern Mexico along the U.S. border. Further, in an illegal marketplace, such as that of illicit drugs, where prices and profits are elevated due to the risks of operating outside the law, violence or the threat of violence becomes the primary means for settling disputes.[105] This has generated concern among U.S. policy makers that the violence in Mexico might spill over into the United States. U.S. officials deny that the drug trafficking-related violence in Mexico has resulted in a spillover into the United States, but they acknowledge that the prospect is a concern.[106]

[102] United States Governmental Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, GAO-12-303, February 2012.

[103] For additional information on preparedness grant consolidation, see "Consolidation of DHS State and Local Programs" in this report.

[104] Homicide levels in Mexico—"largely attributable to drug trafficking and organized crime"—began an escalated climb after 2007. There is debate as to whether this violence leveled off or slightly decreased in 2012; nonetheless, researchers have noted that the violence remains "elevated." University of San Diego, Trans-Border Institute, Drug Violence in Mexico: Data and Analysis Through 2012, February 2013, pp. 1, 11.

[105] Jeffrey A. Roth, "Psychoactive Substances and Violence," National Institute of Justice (Research in Brief Series), February 1994 (Washington, DC: U.S. Department of Justice).

[106] Ramon Bracamontes, "CBP Chief Assesses the Border: Alan Bersin, in El Paso, Assures Safety, Backs Mexico's Fight," *El Paso Times*, January 6, 2011.

Mexican DTOs are reportedly the greatest drug trafficking threat to the United States.[107] Mexican DTOs either (1) transport or (2) produce and transport drugs north across the United States-Mexico border. After being smuggled across the border by DTOs, the drugs are distributed and sold within the United States. The illicit proceeds may then be laundered or smuggled south across the border. The proceeds may also be used to purchase weapons in the United States that are then smuggled into Mexico. The United States is the largest marketplace for illegal drugs and sustains a multi-billion dollar market in illegal drugs—thus partially fueling the threat posed by the DTOs.[108] While drugs are the primary goods trafficked by the DTOs, they also generate income from other illegal activities, such as the smuggling of humans and weapons, counterfeiting and piracy, kidnapping for ransom, and extortion. Reports of these crimes in the United States have contributed to the fear of spillover violence.[109]

One issue that may be of concern to Congress involves determining exactly what constitutes spillover violence above and beyond the level of drug trafficking-related violence that has previously existed in the United States. The interagency community has defined "spillover violence" as violence targeted primarily at civilians and government entities—excluding trafficker-on-trafficker violence[110]—while other experts and scholars have maintained that trafficker-on-trafficker violence is central to spillover.[111] A clear definition of spillover that can be used to track and analyze trends is central to debating policy options to prevent or mitigate such violence.[112] A related issue that Congress may consider is how to prevent drug trafficking-related violence in Mexico from spilling into the United States. Potential options that experts have presented include increasing border enforcement efforts; providing additional aid to Mexico to support the disruption of organized crime, implementation of judicial reform, enhancement of a 21st century border, and strengthening communities;[113] reducing drug demand in the United States; and decriminalizing or legalizing certain drugs.

[107] U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2010,* Product No. 2010-Q0317-001, February 2010, http://www.justice.gov/ndic/pubs38/38661/38661p.pdf.

[108] Oriana Zill and Lowell Bergman, "Do the Math: Why the Illegal Drug Business is Thriving," *PBS Frontline*, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/.

[109] Elyssa Pachio, "Trial of Rogue Tijuana Gang Raises Question of Violence Spilling Over to San Diego," *InSight Crime*, March 5, 2012.

[110] According to the DEA, "[S]pillover violence entails deliberate, planned attacks by the cartels on U.S. assets, including civilian, military, or law enforcement officials, innocent U.S. citizens, or physical institutions such as government buildings, consulates, or businesses. This definition does not include trafficker on trafficker violence, whether perpetrated in Mexico or the U.S." See Drug Enforcement Administration, *Statement of Joseph M. Arabit Special Agent in Charge, El Paso Division*, Regarding "Violence Along the Southwest Border" Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science and Related Agencies, March 24, 2009, http://www.usdoj.gov/dea/speeches/s032409.pdf.

[111] Testimony by David Shirk, Director, Trans-Border Institute, University of San Diego, before the U.S. Congress, House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, *Federal Law Enforcement Response to US-Mexico Border Violence*, 111th Cong., 1st sess., March 24, 2009.

[112] See CRS Report R41075, *Southwest Border Violence: Issues in Identifying and Measuring Spillover Violence* by Kristin M. Finklea. See also U.S. Government Accountability Office, *Southwest Border Security: Data Are Limited and Concerns Vary About Spillover Crime Along the Southwest Border*, GAO-13-175, February 2013.

[113] For more information on U.S. assistance to Mexico and on bilateral security cooperation, see CRS Report R41349, *U.S.-Mexican Security Cooperation: The Mérida Initiative and Beyond*, by Clare Ribando Seelke and Kristin Finklea.

Illicit Proceeds and the Southwest Border

Kristin M. Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

The flow of money outside legal channels not only presents challenges to law enforcement, but it also has a significant nexus with homeland security policy. Proceeds from illegal enterprises are sometimes used to fund broader destabilizing activities, such as smuggling, illegal border crossings, or more violent activities, such as the operations of the FARC (Revolutionary Armed Forces of Colombia) and right-wing paramilitary groups in Colombia.[114] While this is an issue with a global scope, this section focuses specifically on the policies affected by movement of illicit funds across the Southwest border.

The sale of illegal drugs in the United States generates somewhere between $18 billion and $39 billion in annual wholesale proceeds for Mexican and Colombian drug trafficking organizations (DTOs).[115] Money from the DTOs' illegal sale of drugs in the United States is moved south across the border into Mexico. Moving these funds from the United States into Mexico fuels the drug traffickers' criminal activities. This money is not directly deposited into the U.S. financial system, but rather is illegally laundered through mechanisms such as bulk cash smuggling and the Black Market Peso Exchange,[116] or placed in financial institutions, cash-intensive front businesses, prepaid or stored value cards, or money services businesses.[117]

The development of new technologies has provided outlets through which DTOs may conceal their illicit proceeds.[118] Increasingly, the use of stored value cards,[119] mobile banking systems, and other technologies allows traffickers to move profits more quickly and stealthily. In addition, profits that the Mexican DTOs generate from the sale of Colombian cocaine can be moved directly from the United States to the source country without traversing through middlemen.[120]

[114] Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2009*, U.S. Department of State, Washington, DC, August 5, 2010, http://www.state.gov/s/ct/rls/crt/2009/140888.htm.

[115] U.S. Department of Justice, National Drug Intelligence Center (NDIC), *National Drug Threat Assessment 2009,* Product No. 2008-Q0317-005, December 2008, p.49, http://www.usdoj.gov/ndic/pubs31/31379/31379p.pdf. This is the most recent estimate of total annual proceeds. With respect to bulk cash, the most recent NDIC threat assessment (2010) indicates that from 2003 to 2004, an estimated $17.2 billion was smuggled from the United States to Mexico in the form of bulk cash alone. See U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2010,* Product No. 2010-Q0317-001, February 2010, p. 47, http://www.justice.gov/ndic/pubs38/38661/38661p.pdf. (Hereinafter *NDTA, 2010*).

[116] The Department of the Treasury defines the BPME as "a large-scale money laundering system used to launder proceeds of narcotic sales in the United States by Latin American drug cartels by facilitating swaps of dollars in the U.S. for pesos in Colombia through the sale of dollars to Latin America businessmen seeking to buy U.S. goods to export," http://www.fincen.gov/statutes_regs/guidance/html/advis04282006.html.

[117] According to the Department of the Treasury, a money services business is any person or entity engaging in activities including exchanging currency; cashing checks; issuing, selling, or redeeming travelers' checks, money orders, or stored value cards; and transmitting money. For more information, see http://www.fincen.gov/financial_institutions/msb/definitions/msb.html.

[118] See *NDTA, 2010*, pp. 47–50 for more information on developments in illicit finance.

[119] According to the Code of Federal Regulations, stored value are "funds or monetary value represented in digital electronics format (whether or not specially encrypted) and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically," 31 C.F.R. §103.11(vv).

[120] Douglas Farah, "Money Laundering and Bulk Cash Smuggling: Challenges for the Mérida Initiative," in *Shared Responsibility: U.S.-Mexico Policy Options for Confronting Organized Crime*, ed. Eric L. Olson, David A. Shirk, and Andrew D. Selee (2010), p. 144.

While bulk cash smuggling has been an important means by which criminals have moved illegal profits from the United States into Mexico, traffickers have also turned to stored value cards to move money. With these cards, criminals are able to avoid the reporting requirement under which they would have to declare any amount over $10,000 in cash moving across the border. Current federal regulations regarding international transportation only apply to monetary instruments as defined under the Bank Secrecy Act (BSA).[121] A stored value card is not, however, considered a monetary instrument under current law, and thus is not subject to these international transportation regulations. The Financial Crimes Enforcement Network (FinCEN) has issued a proposed rule that would amend the definition of "monetary instrument," for the purposes of BSA international monetary transport regulations, to include prepaid access devices.[122] Policy makers may debate the proper balance between providing for the ease of legitimate monetary transactions and inhibiting the movement of proceeds from illegal activities.

Various departments and agencies—including the Drug Enforcement Administration, Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and FinCEN—share responsibility for combating drug-related activity and the flow of illicit proceeds both along the Southwest border and throughout the United States. Many of these agencies are also represented in Mexico, increasing U.S.-Mexican bilateral cooperation. Further, while some efforts explicitly target money laundering and bulk cash smuggling, other efforts are more tangentially related. For instance, operations targeting southbound firearms smuggling may intercept individuals smuggling not only weapons, but cash proceeds from illicit drug sales as well.

Cross-Border Smuggling Tunnels

Kristin M. Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

Mexican traffickers rely on cross-border tunnels to smuggle persons and drugs, as well as other contraband, from Mexico into the United States. The use of smuggling tunnels has increased not only in frequency but in the sophistication of the tunnels themselves.[123] More than 150 tunnels have been discovered along the Southwest border since the 1990s;[124] notably, there has been an 80% uptick in tunnels detected since 2008.[125] Early tunnels were rudimentary "gopher hole" tunnels dug on the Mexican side of the border, traveling just below the surface, and popping out

[121] 31 U.S.C. §5312(a)(3) defines a monetary instrument as "(A) United States coins and currency; (B) as the Secretary may prescribe by regulation, coins and currency of a foreign country, travelers' checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which title is passed on delivery, and similar material; and (C) as the Secretary of the Treasury shall provide by regulation for purposes of sections 5316 and 5331, checks, drafts, notes, money orders, and other similar instruments which are drawn on or by a foreign financial institution and are not in bearer form."

[122] Department of the Treasury, "Bank Secrecy Act Regulations Definition of "Monetary Instrument," 76 Federal Register 64049, October 17, 2011. Entities such as the Senate Caucus on International Narcotics Control have urged the Administration to finalize this rule. See, for instance, Senate Caucus on International Narcotics Control, The Buck Stops Here: Improving U.S. Anti-Money Laundering Practices, April 2013.

[123] Ken Stier, "Underground Threat: Tunnels Pose Trouble from Mexico to Middle East," *Time*, May 2, 2009.

[124] Statement of James A. Dinkins, Executive Associate Director, Homeland Security Investigations, U.S. Immigration and Customs Enforcement, before the U.S. Congress, Senate United States Senate Caucus on International Narcotics Control, *Illegal Tunnels on the Southwest Border*, 112th Cong., 1st sess., June 15, 2011.

[125] Department of Homeland Security, Office of Inspector General, "CBP's Strategy to Adress Illicit Cross-Border Tunnels," http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-132_Sep12.pdf.

on the U.S. side as close as 100 feet from the border. Slightly more advanced tunnels relied on existing infrastructure, which may be shared by neighboring border cities such as Nogales, AZ, in the United States and Nogales, Sonora, in Mexico. These interconnecting tunnels may tap into storm drains or sewage systems, allowing smugglers to move drugs further and more easily than in tunnels they dug themselves. The most sophisticated tunnels can have rail, ventilation, and electrical systems. One of the most elaborate and sophisticated of such tunnels discovered to date was found in November 2011 in San Diego, CA. It stretched 612 yards in length, boasted electric rail cars, lighting, reinforced walls, and wooden floors, and its discovery resulted in the seizure of 32 tons of marijuana.[126] In July 2012, three sophisticated drug smuggling tunnels were uncovered along the Southwest border in less than a week.[127]

U.S. law enforcement uses various tactics to detect these cross-border tunnels. Law enforcement may use sonic equipment to detect the sounds of digging and tunnel construction and seismic technology to detect blasts that may be linked to tunnel excavation. Another tool for tunnel detection is ground penetrating radar.[128] However, factors including soil conditions, tunnel diameter, and tunnel depth can limit the effectiveness of this technology.

Despite these tools, U.S. officials have acknowledged that law enforcement currently does not have technology that is reliably able to detect sophisticated tunnels.[129] Rather, tunnels are more effectively discovered as a result of human intelligence and tips. U.S. officials have noted the value of U.S.-Mexican law enforcement cooperation in detecting, investigating, and prosecuting the criminals who create and use the cross-border tunnels.[130] As a result, the 113th Congress may not only consider how to best help U.S. law enforcement develop technologies that can keep pace with tunneling organizations, but also examine whether existing bi-national law enforcement partnerships are effective and whether they may be improved to enhance investigations of transnational criminals.

Cargo Security

Marc R. Rosenblum, Specialist in Immigration Policy (mrosenblum@crs.loc.gov, 7-7360)

For more information, see CRS Report R43014, *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*.

Approximately 25 million cargo containers arrived at U.S. ports of entry (POE) in FY2012, down from a high point of 26 million in 2006, but up 4% over FY2011.[131] U.S. Customs and Border

[126] U.S. Drug Enforcement Administration, "Second Major Cross-Border Drug Tunnel Discovered South of San Diego This Month: Investigators Seize 32 Tons of Marijuana, Arrest 6 Suspects," press release, November 30, 2011, http://www.justice.gov/dea/divisions/sd/2011/sd113011.shtml.

[127] Elliot Spagat and Jacques Billeaud, "Drug Tunnels Discovered Between U.S.-Mexico Border Contained Railcar System, Tons Of Pot," *Huffington Post*, July 13, 2012.

[128] For more information, see http://www.geophysical.com/militarysecurity.htm.

[129] Statement of Laura E. Duffy, U.S. Attorney, Southern District of California, U.S. Department of Justice, before the U.S. Congress, Senate United States Senate Caucus on International Narcotics Control, *Illegal Tunnels on the Southwest Border*, 112th Cong., 1st sess., June 15, 2011.

[130] Ibid.

[131] CRS analysis of data provided by U.S. Customs and Border Security (CBP) Office of Legislative Affairs, August 23, 2012 and from U.S. Customs and Border Protection (CBP), "CBP's 2012 Fiscal Year in Review," February 1, 2013, http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/02012013_3.xml.

Protection (CBP), within the Department of Homeland Security (DHS), is America's primary trade enforcement agency, and CBP seeks to balance the benefits of efficient trade flows against the demand for cargo security and the enforcement of U.S. trade laws. Thus, the overarching policy question with respect to incoming cargo is how to minimize the risk that weapons of mass destruction (WMD), illegal drugs, and other contraband will enter through a U.S. port of entry (POE), while limiting the costs and delays associated with such enforcement. Six laws enacted between 2002 and 2007 included provisions related to the trade process and cargo security.[132]

CBP's current trade strategy emphasizes "risk management" and a "multi-layered" approach to enforcement.[133] With respect to cargo security, risk management means that CBP segments importers into higher and lower risk pools and focuses security procedures on higher-risk flows, while expediting lower-risk flows. CBP's "multi-layered approach" means that enforcement occurs at multiple points in the import process, beginning before goods are loaded in foreign ports and continuing months or years after the time goods have been admitted into the United States. In recent years, congressional attention to cargo security has focused on one of CBP's primary tools for risk management, the Customs-Trade Partnership Against Terrorism (C-TPAT) trusted trader program, and on the statutory requirement that 100% of incoming maritime cargo containers be scanned abroad prior to being loaded on U.S.-bound ships. Congress also faces perennial questions about spending levels on POE infrastructure and personnel.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary public-private and international partnership that permits certain import-related businesses to register with CBP and perform security tasks prescribed by the agency. In return C-TPAT members are recognized as low-risk actors and are eligible for expedited import processing and other benefits.[134] CBP established C-TPAT in November 2001 following the September 11, 2001 (9/11), terrorist attacks, and the program was authorized as part of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act, P.L. 109-347).

Some Members of Congress and some CBP officials favor increased participation in C-TPAT and related programs as a way to facilitate legal trade flows.[135] Yet some businesses have criticized the program for providing inadequate membership benefits, especially in light of the time and

[132] The Trade Act of 2002 (P.L. 107-210), the Maritime Transportation Security Act of 2002 (P.L. 107-295), the Homeland Security Act of 2002 (P.L. 107-296), the Coast Guard and Maritime Transportation Act of 2004 (P.L. 108-293), the Security and Accountability for Every Port Act of 2006 (SAFE Port Act, P.L. 109-347), and the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act, P.L. 110-53).

[133] See CBP, *CBP Trade Strategy: Fiscal Years 2009-2013*, Washington, DC, 2009, http://www.cbp.gov/linkhandler/cgov/trade/trade_outreach/trade_strategy/cbp_trade_strategy.ctt/cbp_trade_strategy.pdf.

[134] See U.S. CBP, "C-TPAT: Program Overview," http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_program_information/what_is_ctpat/ctpat_overview.ctt/ctpat_overview.pdf. Commercial truck drivers who are Customs-Trade Partnership Against Terrorism (C-TPAT) members also are eligible to join the Free and Secure Trade System (FAST), which permits expedited processing at land ports of entry; and C-TPAT members who are residents of the United States and are known importers that have businesses physically established, located, and managed within the United States may be eligible for the Importer Self-Assessment Program (ISA), which exempts importers from certain post-entry enforcement audits. See ibid., and U.S. Customs and Border Protection, "Fact Sheet: Fast and Secure Trade," http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/fast/fast_fact.ctt/fast_fact.pdf.

[135] See for example, U.S. Congress, House Committee on Ways and Means, Subcommittee on Trade, *Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and Enforcement*, 112th Cong., 2nd sess.. May 17, 2012.

financial investments required to become certified as C-TPAT members.[136] In particular, even with expedited processing, C-TPAT members may face delays during the import process as a result of limited coordination between CBP and the other 46 government agencies that play a role in trade enforcement. Thus, while many large import-related businesses have joined C-TPAT, the Congressional Research Service (CRS) estimates that only about 6% of all eligible import-related businesses and about 8% of eligible customs brokers have joined the program.[137] Congress may consider legislation to increase C-TPAT benefits or take other steps to encourage C-TPAT participation and thereby facilitate lawful trade flows.[138]

Yet there may be no easy way to substantially expand C-TPAT benefits. In the case of land ports, the primary trusted trader benefit is access to dedicated lanes where wait times may be shorter and more predictable. But adding lanes at land ports is difficult because many of them are located in urban areas with limited space for expansion and with limited ingress and egress infrastructure.[139] In the case of maritime imports, the primary trusted trader benefit is a reduced likelihood of secondary inspection.[140] But only about 4% of all maritime containers currently are selected for such an inspection,[141] so C-TPAT membership may offer little practical advantage in this regard. In addition, some CBP officials have told CRS that further reduction in C-TPAT inspections may raise security risks because smugglers may establish clean companies and join the program in order to game the system.[142]

100% Scanning Requirement

Section 231 of the SAFE Port Act directed the Department of Homeland Security (DHS), in coordination with the Department of Energy (DOE), the private sector, and foreign governments, to pilot an integrated system in three foreign ports to scan 100% of cargo containers destined for the United States from those ports.[143] Section 232 of the law required that 100% of cargo

[136] Ibid.

[137] As of August 22, 2012, 10,337 businesses had joined C-TPAT, including 845 customs brokers, according to data provided by CBP Office of Legislative Affairs, August 24, 2012. By comparison, U.S. Census data indicates that there were 181,648 U.S. importers in 2010 and CBP data indicate that there were 11,000 customs brokers; see U.S. Census, "A Profile of U.S. Importing and Exporting Companies, 2009-2010," http://www.census.gov/foreign-trade/Press-Release/edb/2010/edbrel.pdf; and CBP, "Becoming a Customs Broker," http://www.cbp.gov/xp/cgov/trade/trade_programs/broker/brokers.xml. Nonetheless, data from the CBP Office of Legislative Affairs also indicate that C-TPAT members account for 50-56% of all imports by value.

[138] See for example, §§201-202 of the Trade Facilitation and Trade Enforcement Reauthorization Act of 2013 (S. 662/H.R. 3004), which would direct CBP to consult with private sector entities and coordinate with other federal agencies to ensure that participants in trusted trader programs "receive commercially significant and measurable trade benefits." Certain C-TPAT benefits are described in statute under §§213-216 of the SAFE Port Act of 2006.

[139] See U.S. Department of Commerce, *Draft Report: Improving Economic Outcomes by Reducing Border Delays*, Facilitating the Vital Flow of Commercial Traffic Across the US-Mexican Border, Washington, DC, 2008, http://grijalva.house.gov/uploads/Draft%20Commerce%20Department%20Report%20on%20Reducing%20Border%20Delays%20Findings%20and%20Options%20March%202008.pdf.

[140] Secondary inspection may include both non-intrusive imaging (NII) scans and/or physical inspection, in which the container may be opened and unpacked so that materials can be examined.

[141] CRS analysis of data provided by U.S. Customs and Border Security (CBP) Office of Legislative Affairs, August 23, 2012.

[142] Also see Tony Payan, *The Three U.S.-Mexico Border Wars: Drugs, Immigration, and Homeland Security* (Westport, CT: Praeger, 2006), pp. 34-36.

[143] The 100% scanning pilot program is known as the Secure Freight Initiative (SFI). Following DHS's evaluation of (continued...)

containers imported into the United States be *screened* by DHS to identify high-risk containers, and that 100% of containers identified as high risk also be *scanned* through non-intrusive inspection (NII) and radiation detection equipment before arriving in the United States.[144] In 2007, Section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) (P.L. 110-53) amended the SAFE Port Act to require that by July 1, 2012, 100% of maritime containers imported to the United States—that is, from all ports, whether or not they are identified as high-risk—be scanned by NII and radiation detection equipment before being loaded onto a U.S.-bound vessel in a foreign port. Nonetheless, as of August 2012, just 1% of cargo was scanned with NII before being loaded on U.S.-bound ships—and only about 5% of cargo was subject to NII scanning at any point prior to entering the United States.[145]

On May 2, 2012, DHS Secretary Janet Napolitano notified Members of Congress that she would exercise her authority under the 9/11 Act to extend the deadline for 100% scanning.[146] The decision to delay implementation of the 100% scanning program partly reflects the department's findings from its evaluation of the pilot program. In its final report to Congress on the program, CBP identified three main obstacles to implementing 100% scanning at all foreign ports.[147] First, 100% scanning requires significant host state and private sector cooperation, but some foreign governments and business groups do not support 100% scanning. Second, 100% scanning would be logistically difficult. Initial pilots were deployed in relatively low-volume ports with natural chokepoints, but many cargo containers pass through large volume ports with more varied port architectures. Third, 100% scanning would be costly. In February 2012, the Congressional Budget Office (CBO) estimated that 100% scanning at foreign ports would cost an average of $8 million per shipping lane to implement, or a total of about $16.8 billion for all 2,100 shipping lanes.[148] Port operators and foreign partners also absorb additional costs associated with fuel and utilities, staffing, and related expenses. More generally, 100% scanning conflicts with DHS's overall

(...continued)

the SFI in 2012, the program was scaled back to a single port, Port Qasim, in Pakistan.

[144] The risk-based scanning program is known as the Container Security Initiative (CSI).

[145] CRS analysis of data provided by U.S. Customs and Border Security (CBP) Office of Legislative Affairs, August 23, 2012.

[146] Letter from Janet Napolitano, Secretary of Homeland Security, to Hon. Joseph I. Lieberman, Senator, May 2, 2012. The 9/11 Act permits the Secretary to extend the deadline by two years and in additional two-year increments by certifying that two of the following conditions exist: that scanning systems are not available, are insufficiently accurate, cannot be installed, cannot be integrated with existing systems, will significantly impact trade and the flow of cargo, and/or do not provide adequate notification of questionable or high-risk cargo. In her notification to Congress, Secretary Napolitano certified that the use of systems to scan containers would have a significant and negative impact on trade capacity and cargo flows, and that systems to scan containers cannot be purchased, deployed, or operated at overseas ports due to limited physical infrastructure.

[147] See U.S. CBP, Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, §231). Also see U.S. GAO, Supply Chain Security: Container Secuirty Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning, GAO-12-422T, February 7, 2012, http://www.gao.gov/assets/590/588253.pdf. Also see letter from Janet Napolitano, Secretary of Homeland Security, to Hon. Joseph I. Lieberman, Senator, May 2, 2012.

[148] Spoken response by Kevin McAleenan, Acting Assistant Commissioner, Office of Field Operations, U.S. CBP, U.S. Department of Homeland Security, before the Border and Maritime Security Subcommittee of the Homeland Security Committee, U.S. House, hearing "Balancing Maritime Security and Trade Facilitation: Protecting our Ports, Increasing Commerce and Securing the Supply Chain - Part I," February 7, 2012. CBP reports that the U.S. government spent a total of about $120 million during the first three years of the Secure Freight Initiative; CBP, *Report to Congress on Integrated Scanning System Pilots*, p. 13.

approach to risk management, which seeks to focus scarce inspection resources on the highest-risk containers.[149]

Some Members of Congress have expressed frustration that DHS has made little progress toward implementing 100% scanning.[150] Congress may continue to monitor the 100% scanning requirement and encourage DHS to scan a higher proportion of inbound cargo. On the other hand, in light of the difficulties DHS has identified, Congress may consider changes to the 100% scanning requirement, potentially including provisions to allow DHS to scan less than 100% of U.S.-bound cargo or to allow certain scanning to occur within U.S. ports rather than abroad. In its report to accompany the Department of Homeland Security Appropriations Bill, 2014 (H.R. 2217), the House Appropriations Committee directed DHS, in light of the department's finding that 100% scanning is cost-prohibitive, to submit an alternative strategy for cargo scanning to Congress by January 1, 2014.[151]

Port of Entry (POE) Infrastructure and Personnel

In light of the substantial flow of cargo and travelers at ports of entry (also see "Immigration Inspections at Ports of Entry"), one perennial issue for Congress is how to allocate resources for CBP Office of Field Operations (OFO) personnel and for port infrastructure. Some in Congress have argued that inadequate personnel and infrastructure have contributed to costly delays and unpredictable wait times at ports of entry, particularly at land ports on the U.S.-Mexico border.[152] In general, Congress has invested more heavily since 2011 in enforcement personnel between ports of entry (i.e., U.S. Border Patrol agents) than in OFO officers (also see "Enforcement between Ports of Entry").[153] The Obama Administration's FY2014 budget request proposed to increase OFO personnel by 3,477 officers (on top of 21,775 officers deployed in FY2013) through a combination of appropriations and increased user fees, but the House-passed DHS appropriations act (H.R. 2217) included funding for only about 800 new officers, while the Senate-reported version of the bill would support 1,850 officers.[154] Other legislation under consideration in both chambers also would require CBP to deploy additional officers at POEs.[155]

DHS also has proposed to expand POE inspection services while controlling costs by forming public-private partnerships (PPPs) with private sector and/or sub-federal government agencies to support customs and immigration services at certain ports of entry. Current law generally prohibits Customs and Border Protection from receiving reimbursement for POE services or from

[149] See U.S. CBP, "CBP Trade Strategy: Fiscal Years 2009-2013," Washington, DC: 2009.

[150] See for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce, and Securing the Supply Chain - Part I*, 112th Cong., 2nd sess., February 7, 2012.

[151] H.Rept. 113-91, p. 32.

[152] See, for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Using Technology to Facilitate Trade and Enhance Security at Our Ports of Entry*, 112th Cong., 2nd sess., May 1, 2012. On border wait times, also see GAO, *CBP Action Needed to Improve Wait Time Data and Measure Outcomes of Trade Facilitation Effort*, GAO-13-603, July 24, 2013.

[153] According to a CRS analysis of data provided by CBP Office of Congressional Affairs in January 2013, staffing for enforcement between ports of entry more than doubled between FY2004 and FY2012 (increasing from 10,819 to 21,394), while staffing at ports of entry increased just 20% during this period (from 18,110 to 21,790).

[154] H.Rept. 113-91, pp. 30-31; S.Rept. 113-77, p. 33.

[155] See for example the Border Security, Economic Opportunity, and Immigration Modernization Act (S. 744), as passed by the Senate, and the Putting Our Resources Toward Security (PORTS) Act (H.R. 583).

collecting extra fees as compensation for providing services outside of normal business hours, and so limits CBP's authority to form such partnerships.[156] But pursuant to the Administration's FY2013 budget request, section 560 of the FY2013 DHS appropriations act (Division D of P.L. 113-6) established a pilot program to permit CBP to enter into up to five PPPs to support customs and immigration services at certain ports of entry. The Administration's FY2014 request included similar language regarding five pilot projects, and requested authority to expand the partnerships program by permitting DHS to accept donations of real and personal property (including monetary donations) from private parties and state and local government entities for the purpose of constructing or expanding POE facilities. The House-passed Department of Homeland Security Appropriations Act, 2014 (H.R. 2217) does not include language supporting the Administration's request, and the Trade Facilitation and Trade Enforcement Reauthorization Act of 2013 (S. 662/H.R. 3004) would strike the existing pilot program. On the other hand, the Senate-reported version of H.R. 2217 would reauthorize the PPP pilot program, and also would meet the Administration's request to authorize CBP to accept donations for the purpose of constructing or operating POEs.[157]

Domestic Nuclear Detection

Dana A. Shea, Specialist in Science and Technology Policy (dshea@crs.loc.gov, 7-6844)

Congress has emphasized the need to detect and interdict smuggled nuclear and radiological material before it enters the United States, funding investment in nuclear detection domestically and abroad. DHS has adopted a strategy of securing the border through emplacement of radiation portal monitors and non-intrusive imaging equipment. Some experts have criticized this combined system as insufficient to detect all smuggled special nuclear material. DHS has spent several years developing, testing, and evaluating next-generation detection equipment. Several of these next-generation systems, the Advanced Spectroscopic Portal and the Cargo Advanced Automated Radiography System, did not meet testing and evaluation milestones, lagged performance and timeline expectations, and ultimately were not procured.[158]

DHS has deployed radiation portal monitors and other nuclear and radiological material detection equipment since its establishment. In 2005, DHS established a new office, the Domestic Nuclear Detection Office (DNDO), to research, develop, and procure needed necessary detection equipment and coordinate DHS nuclear detection activities located mainly in Customs and Border Protection, U.S. Coast Guard, and the Transportation Security Administration. The Government Accountability Office (GAO) and other groups have questioned the efficacy of DNDO's efforts to develop a next-generation radiation detection system.

[156] 19 U.S.C. §58b restricts CBP's authority to receive reimbursement to cases in which the volume or value of business cleared through the port is too low to justify the availability of customs services and if the governor of the state in which the port is located approves the arrangement; and 19 U.S.C. §1451 restricts CBP's ability to collect extra fees as compensation for providing services outside of normal business hours.

[157] Also see CRS Report R43147, *Department of Homeland Security: FY2014 Appropriations*, coordinated by William L. Painter.

[158] For a brief overview of challenges with the Advanced Spectroscopic Portal and the Cargo Advanced Automated Radiography System, see Government Accountability Office, *Combating Nuclear Smuggling: DHS Has Developed a Strategic Plan for Its Global Nuclear Detection Architecture, but Gaps Remain*, GAO-11-869T, July 26, 2011.

As mentioned in the preceding section, Congress also has required DHS to scan all containerized cargo entering the United States for nuclear and radiological material. DHS has not yet met this requirement, and stakeholders question whether the DHS approach will meet this requirement in the future. In addition, a shortfall of a key neutron detection material, helium-3, has forced a reconsideration of the current nuclear detection approach.[159] DHS has invested in testing new neutron-detection materials and refitting deployed systems with alternative neutron-detection capabilities. As currently deployed systems approach their design lifetime, DHS and congressional decision-makers face questions whether to recapitalize these systems or further invest in next-generation technology.

DHS activities to detect smuggled radiological and nuclear materials at the U.S. border are part of a large interagency effort to develop a global nuclear detection architecture (GNDA). Congress made DHS, through DNDO, responsible for coordinating federal efforts within the GNDA and implementing this architecture domestically. A GNDA strategic plan has been released, and DHS has developed an implementation plan for its portion of the GNDA.[160] Other agencies have not yet developed equivalent implementation plans. While GAO has identified weaknesses in the GNDA strategic plan, it has also generally supported DHS's development of an implementation plan.

The 113th Congress may continue its oversight over the development, testing, and procurement of current and next-generation nuclear detection equipment, interagency coordination in nuclear detection, the sufficiency of the global nuclear detection architecture that links this equipment together, and DHS's approach to the helium-3 shortage.

Transportation Worker Identification Credential (TWIC)

John Frittelli, Specialist in Transportation Policy (jfrittelli@crs.loc.gov, 7-7033)

For more information, see CRS Report RL33512, *Transportation Security: Issues for the 113th Congress*.

On January 25, 2007, TSA and the Coast Guard issued a final rule implementing the TWIC at U.S. ports.[161] Longshoremen, port truck drivers, railroad workers, merchant mariners, and other workers at a port must apply for a TWIC card to obtain unescorted access to secure areas of port facilities or vessels. The card was authorized under the Maritime Transportation Security Act of 2002 (MTSA, §102 of P.L. 107-295). Since October 2007, when TSA began issuing TWICs, about 2.3 million maritime workers have obtained a card. The card must be renewed every five years, so many workers must renew their cards for the first time.

TSA conducts a security threat assessment of each worker before issuing a card. The security threat assessment uses the same procedures and standards established by TSA for truck drivers

[159] See CRS Report R41419, *The Helium-3 Shortage: Supply, Demand, and Options for Congress*, by Dana A. Shea and Daniel Morgan for background.

[160] See Gowadia, Dr. Huban, written testimony in his capacity as Acting Director, Domestic Nuclear Detection Office, before the House Committee on Homeland Security, Subcommittee on Infrastructure Protection, and Security Technologies, "Preventing Nuclear Terrorism: Does DHS have an Effective and Efficient Nuclear Strategy," July 26, 2012.

[161] *Federal Register*, v. 72, no. 16, January 25, 2007, pp. 3492 - 3604. Codified at 49 CFR 1572.

carrying hazardous materials, including examination of the applicant's criminal history, immigration status, and possible links to terrorist activity to determine whether a worker poses a security threat. A worker pays a fee of about $130 that is intended to cover the cost of administering the cards. A worker must visit an enrollment site twice, once to apply for the card and provide biometric information and a second time to pick up the card and confirm identification with biometric information.[162]

The card uses biometric technology for positive identification. Terminal operators are to deploy card readers at the gates to their facilities, so that a worker's fingerprint template will be scanned each time he enters the port area and matched to the data on the card. However, despite a statutory deadline of 2009 for issuance of a final rule on card reader deployment, TSA has not yet determined what kind of card reader technology to require.[163] In the absence of card readers, the card is currently being used as a "flash pass," and the biometric data on the card are not being used to positively identify the worker.

In March 2013, the Coast Guard issued a notice of proposed rulemaking (NPRM)[164] in which it proposed requiring card readers only for facilities or vessels handling dangerous bulk commodities (including barge fleeting areas) or facilities handling more than 1,000 passengers at a time – maritime sectors the Coast Guard considers to be of higher risk. The Coast Guard estimates that 38 U.S.-flag vessels and 352 facilities would be required to have card readers, which equates to about 0.3% of the vessels and 16% of the facilities it regulates under MTSA. Other vessels and facilities, including those handling containerized cargo, will continue to use the TWIC as a "flash pass," unless the Coast Guard amends the rulemaking at a future date. The comment period for the NPRM closed on June 20, 2013; the Coast Guard plans to take a year to review the comments.[165]

Recent GAO audits have been highly critical of how TWIC is being implemented. A 2013 audit found that the results of a pilot test of card readers should not be relied upon for developing regulations on card reader requirements because they were incomplete, inaccurate, and unreliable.[166] This audit was discussed at a hearing by the House Subcommittee on Government Operations on May 9, 2013,[167] and by the House Subcommittee on Border and Maritime Security on June 18, 2013.[168] Another 2013 GAO audit examined TSA's Adjudication Center (which

[162] Many workers have objected to the second visit, asking why the card could not be mailed to them. GAO has reported that mailing the card would not meet government standards for issuing security credentials. GAO, *Transportation Worker Identification Credential: Mailing Credentials to Applicants' Residence Would Not Be Consistent with DHS Policy,* GAO-11-542R, April 13, 2011. §709 of the Coast Guard and Maritime Transportation Act of 2012 (P.L. 112-213) changes the process to require only one in-person visit by the applicant.

[163] §104 of the SAFE Port Act (P.L. 109-347) set a deadline of April 13, 2009, for the issuance of a final rule on card reader deployment. See U.S. Congress, House Committee on Transportation and Infrastructure, *A Review of the Delays and Problems Associated with TSA's Transportation Worker Identification Credential*, 112th Cong., 2nd sess., June 28, 2012.

[164] 78 FR 17782, March 22, 2013.

[165] Comments filed can be viewed at http://www.regulations.gov under docket # USCG-2007-28915.

[166] GAO, *Transportation Worker Identification Credential – Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed,* GAO-13-198, May 8, 2013.

[167] U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on Government Operations, *Federal Government Approaches to Issuing Biometric IDs*, 113th Cong., 1st sess., May 9, 2013.

[168] U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Threat, Risk and Vulnerability: the TWIC Program*, 113th Cong., 1st sess., June 18, 2013.

performs security threat assessments on TWIC applicants and other transportation workers) and recommended steps the agency could take to better measure the Center's performance.[169] A 2011 audit found internal control weaknesses in the enrollment, background checking, and use of the TWIC card at ports, which were said to undermine the effectiveness of the credential in screening out unqualified individuals from obtaining access to port facilities.[170]

Aviation Security

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

Following the 9/11 terrorist attacks, Congress took swift action to create the Transportation Security Administration (TSA), federalizing all airline passenger and baggage screening functions and deploying large numbers of armed air marshals on commercial passenger flights. Despite extensive focus on aviation security over the past decade, a number of challenges remain, including:

- Effectively screening passengers, baggage, and cargo for explosive threats;
- Developing effective risk-based methods for screening passengers and others with access to aircraft and sensitive areas;
- Exploiting available intelligence information and watchlists to identify individuals that pose potential threats to civil aviation;
- Developing effective strategies for addressing aircraft vulnerabilities to shoulder-fired missiles and other standoff weapons; and
- Addressing the potential security implications of unmanned aircraft operations in domestic airspace.

Explosives Screening Strategy for the Aviation Domain

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

For additional information, see CRS Report R41515, *Screening and Securing Air Cargo: Background and Issues for Congress*, and CRS Report R42750, *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening* .

Prior to the 9/11 attacks, explosives screening in the aviation domain was limited in scope and focused on selective screening of checked baggage placed on international passenger flights. Immediately following the 9/11 attacks, the Aviation and Transportation Security Act (ATSA, P.L. 107-71) mandated 100% screening of all checked baggage placed on domestic passenger flights and on international passenger flights to and from the United States. In addition, the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53) mandated the physical screening of all cargo placed on passenger flights. While TSA has met the requirement

[169] GAO, *Transportation Security: Action Needed to Strengthen TSA's Security Threat Assessment Process,* GAO-13-629, July 19, 2013.

[170] GAO, *Transportation Worker Identification Credential – Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, May 2011, GAO-11-657.

for cargo screening domestically, largely through implementation of its Certified Cargo Screening Program to oversee screening at off-airport shipping and consolidation facilities combined with supply chain security measures, additional work is needed to implement similar measures for U.S.-bound international flights. Although TSA has yet to fully implement 100% screening of cargo placed on international flights, recent attention has particularly focused on improving explosives screening of passengers in response to continued threats.

On December 25, 2009, a passenger attempted to detonate an explosive device concealed in his underwear aboard Northwest Airlines flight 253 during its approach to Detroit, MI. Al-Qaeda in the Arabian Peninsula claimed responsibility. Al-Qaeda and its various factions have maintained a particular interest in attacking U.S.-bound airliners. Since 9/11, Al-Qaeda has also been linked to the Richard Reid shoe bombing incident aboard American Airlines flight 63 en route from Paris to Miami on December 22, 2001, a plot to bomb several trans-Atlantic flights departing the United Kingdom for North America in 2006, and the October 2010 plot to detonate explosives concealed in air cargo shipments bound for the United States. In response to the Northwest Airlines flight 253 incident, the Obama Administration accelerated deployment of Advanced Imaging Technology (AIT) whole body imaging (WBI) screening devices and other technologies at passenger screening checkpoints. This deployment responds to the 9/11 Commission recommendation to improve the detection of explosives on passengers.[171]

In addition to AIT, next generation screening technologies for airport screening checkpoints include advanced technology x-ray systems for screening carry-on baggage, bottled liquids scanners, cast and prosthesis imagers, shoe scanning devices, and portable explosives trace detection equipment. The use of AIT has raised a number of policy questions. Privacy advocates have objected to the intrusiveness of AIT, particularly if used for primary screening.[172] The screening of children, the elderly, and individuals with medical conditions and disabilities has been particularly contentious. Recent modifications to pat-down screening procedures, involving more detailed inspection of private areas, have also raised privacy concerns.[173] To allay privacy concerns, TSA required remote screening of images outside of public view and forbade recording or storage of AIT images. Other concerns about AIT included the amount of time it takes to screen passengers and the potential medical risks posed by backscatter x-ray systems, despite assurances that the radiation doses from screening are comparatively small. TSA has also begun implementing automated threat detection capabilities using automated targeting recognition (ATR) software that will eliminate the need for TSA screeners to view AIT-generated images. Because the contractor could not develop ATR software that would work with their AIT units, TSA terminated the contract in January 2013 and began to phase out use of backscatter AIT in favor of millimeter-wave scanning technology that is faster and more compatible with ATR.[174]

Some have advocated for risk-based use of AIT, in coordination with the risk-based approaches to passenger screening discussed below. Some past legislative proposals have specifically sought to prohibit the use of WBI technology for primary screening (see, e.g., H.R. 2200, 111th Congress),

[171] For additional background, see CRS Report R42750, *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening*, by Bart Elias.

[172] See, e.g., American Civil Liberties Union. ACLU Backgrounder on Body Scanners and "Virtual Strip Searches," New York, NY, January 8, 2010.

[173] Donna Goodison, "Passengers Shocked by New Touchy-Feely TSA Screening," *The Boston Herald,* August 24, 2010.

[174] Burns, Bob, The TSA Blog, "Rapiscan Backscatter Contract Terminated—Units to be Removed," January 18, 2013. http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract.html.

while others had sought to accelerate the deployment of ATR software and the phase-out of AIT systems not capable of automated threat detection (see H.R. 3011, 112th Congress).

Risk-Based Passenger Screening

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

TSA has initiated a number of risk-based screening initiatives to focus its resources and apply directed measures based on intelligence-driven assessments of security risk. Initiatives include a new trusted traveler trial program called PreCheck, modified screening procedures for children 12 and under, and a trial program for expedited screening of known flight crew and cabin crew members. Trial programs are also underway for modified screening of elderly passengers similar to those procedures put in place for children. These various trial programs may allow for improved screening efficiencies and potential cost savings.

A cornerstone of TSA's risk-based initiatives is the PreCheck program. PreCheck is TSA's latest version of a trusted traveler program that has been modeled after similar CBP programs including Global Entry, SENTRI, and NEXUS. It is currently available on a trial basis to members of those programs, frequent flyer program members of five major airlines, and, in some cases, to military service members, at a limited number of airports. Children 12 and younger traveling with PreCheck participants are also permitted to travel through the expedited screening lanes. A similar test program, called the Registered Traveler program, which involved private vendors that issued and scanned participants' biometric credentials, was scrapped by TSA in 2009 because it failed to show a demonstrable additional security benefit. Questions remain regarding whether PreCheck will be an effective tool to assist in directing security resources to unknown or elevated risk travelers while expediting the screening of program participant.

One potential concern raised over PreCheck implementation and expedited screening focuses on the public dissemination of instructions, posted on Internet sites, detailing how to read and decipher boarding passes to determine if a passenger has been selected for expedited screening. The lack of encryption has been cited as a potential security weakness that could be exploited to attempt to avoid detection of threat items by more extensive security measures. Other concerns raised over the program include the lack of biometric identity authentication and the lack of detailed background checks, particularly for participants who qualify for PreCheck solely on the basis of their frequent flyer status.[175]

In addition to passenger screening, TSA, in coordination with participating airlines and labor organizations representing airline pilots, has initiated a known crewmember program to expedite security screening of airline flight crews.[176] In July 2012, TSA expanded the program to include flight attendants.[177]

[175] Robert Poole, "Problems and Progress with PreCheck," *Airport Policy and Security News #84,* November 5, 2012, The Reason Foundation, Los Angeles, http://reason.org/news/show/airport-policy-and-security-news-84.

[176] See http://www.knowncrewmember.org/Pages/Home.aspx.

[177] Transportation Security Administration, *Press Release: U.S. Airline Flight Attendants to Get Expedited Airport Screening in Second Stage of Known Crewmember Program,* Friday, July 27, 2012, http://www.tsa.gov/press/releases/2012/07/27/us-airline-flight-attendants-get-expedited-airport-screening-second-stage.

TSA has also developed a passenger behavior detection program to identify potential threats based on observed behavioral characteristics. In addition to employing observational techniques, TSA Behavior Detection Officers are field testing more extensive passenger interviews based on methods employed at Israeli airports.[178] Questions remain regarding the effectiveness of the behavioral detection program, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling of passengers despite concerted efforts to focus solely on behaviors rather than individual passenger traits or characteristics. While TSA has proposed to increase the numbers of Behavior Detection Officers (BDOs) by 72 to 3,131 in FY2013, the House Appropriations Committee did not support this increase, citing TSA's lack of clear evidence that BDOs provide protection against potential aviation security threats. The committee has called for a formal cost-benefit analysis of the BDO program along with a robust risk-based strategy for BDO deployment.[179]

The Use of Terrorist Watchlists in the Aviation Domain

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

For additional information see CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*.

The failed bombing attempt of Northwest Airlines flight 253 on December 25, 2009, also raised policy questions regarding the effective use of terrorist watchlists and intelligence information to identify individuals that may pose a threat to aviation. Specific failings to include the bomber on either the no-fly or selectee list, despite intelligence information suggesting that he potentially posed a security threat, prompted reviews of the intelligence analysis and terrorist watchlisting processes. Adding to these concerns, on the evening of May 3, 2010, Faisal Shazad, a suspect in an attempted car bombing in New York's Times Square, was permitted to board an Emirates Airline flight to Dubai at the John F. Kennedy International airport, even though his name had been added to the no-fly list earlier in the day. He was subsequently identified, removed from the aircraft, and arrested after the airline forwarded the final passenger manifest to CBP's National Targeting Center just prior to departure.[180] Subsequently, TSA modified security directives to require airlines to check passenger names against the no-fly list within two hours of being electronically notified of an urgent update, instead of allowing 24 hours to recheck the list. The event also prompted calls to accelerate the ongoing transfer of watchlist checks from the airlines to the TSA under the Secure Flight program, a process which has now been completed.[181]

By the end of November 2010, DHS announced that 100% of passengers flying to or from U.S. airports are being vetted using the Secure Flight system.[182] Secure Flight continues the no-fly and selectee list practices of vetting passenger name records against a subset of the Terrorist Screening Database (TSDB). On international flights, Secure Flight operates in coordination with the use of watchlists by CBP's National Targeting Center-Passenger, which relies on the Advance

[178] Katie Johnston, "A Question for You," *The Boston Globe,* August 3, 2011.

[179] H.Rept. 112-492, pp. 65-66.

[180] Scott Shane, "Lapses Allowed Suspect to Board Plane," *The New York Times*, May 4, 2010.

[181] See CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*, by William J. Krouse and Bart Elias for additional background.

[182] Department of Homeland Security, "DHS Now Vetting 100 Percent of Passengers On Flights Within Or Bound For U.S. Against Watchlists," Press Release, November 30, 2010.

Passenger Information System (APIS) and other tools to vet both inbound and outbound passenger manifests.

Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 113th Congress include the timeliness of updating watchlists as new intelligence information becomes available; the extent to which complete terrorist information available to the federal government is exploited to assess possible threats among airline passengers and airline and airport workers; the ability to detect potential identity fraud or other attempts to circumvent terrorist watchlist checks, including the potential use of biometrics; the adequacy of established protocols for providing redress to individuals improperly identified as potential threats by watchlist checks; and the adequacy of coordination with international partners.

Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771).

The threat to civilian aircraft posed by shoulder-fired missiles or other standoff weapons capable of downing an airliner remains a vexing concern for aviation security specialists and policymakers. The threat was brought into the spotlight by the November 2002 attack on a chartered Israeli airliner in Mombasa, Kenya. In 2003, then-Secretary of State Colin Powell remarked that there was "no threat more serious to aviation."[183] Since then, Department of State and military initiatives seeking bilateral cooperation and voluntary reductions of man-portable air defense systems (MANPADS) stockpiles have reduced worldwide inventories by at least 32,500 missiles.[184] Despite this progress, an unknown number of such weapons may still be in the hands of insurgents. This threat, combined with the limited capability to improve security beyond airport perimeters and to modify flight paths, leaves civil aircraft vulnerable to missile attacks, especially in conflict zones and other high-risk areas.

The most visible DHS initiative to address the threat was the multiyear Counter-MANPADS program carried out by the DHS Science and Technology Directorate. The program concluded in 2009 with extensive operational and live-fire testing along with FAA certification of systems from two vendors capable of protecting airliners against heat-seeking missiles. The systems have not been operationally deployed on commercial airliners, however, due largely to the high acquisition and life-cycle costs of these units. Some critics have also pointed out that the units do not protect against the full range of potential weapons that pose a potential threat to civil airliners. Proponents, however, argue that the systems do appear to provide effective protection against what is likely the most menacing standoff threat to civil airliners: heat-seeking MANPADS. Nonetheless, the airlines, which continue to face economic difficulties, have not voluntarily invested in these systems for operational use and argue that the costs for such systems should be borne, at least in part, by the federal government. Policy discussions have focused mostly on whether to fund the acquisition of limited numbers of the units for use by the Civil Reserve Aviation Fleet, civilian airliners that can be called up to transport troops and supplies for the military. Other approaches to protecting aircraft, including ground-based missile countermeasures and escort planes or drones equipped with antimissile technology, have been considered on a

[183] Katie Drummond, "Where Have All the MANPADS Gone?" *Wired,* February 22, 2010.

[184] Ibid; U.S. Department of State, Bureau of Political-Military Affairs, *MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense System*, July 27, 2011, http://www.state.gov/t/pm/rls/fs/169139.htm.

more limited basis, but these options face operational challenges that may limit their effectiveness.

At the airport level, improving security and reducing the vulnerability of flight paths to potential MANPADS attacks continues to pose unique challenges. While major airports have conducted vulnerability studies, and many have partnered with federal, state, and local law enforcement agencies to reduce vulnerabilities to some degree, these efforts face significant challenges because of limited resources and large geographic areas where aircraft are vulnerable to attack. While considerable attention has been given to this issue in years past, considerable vulnerabilities remain, and any terrorist attempts to exploit those vulnerabilities could quickly escalate the threat of shoulder-fired missiles to a major national security priority.

Security Issues Regarding the Operation of Unmanned Aircraft

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771); Jeremiah Gertler, Specialist in Military Aviation (jgertler@crs.loc.gov, 7-5107); and Richard M. Thompson II, Legislative Attorney (rthompson@crs.loc.gov, 7-8449)

For more information, see CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*.

Provisions in the FAA Modernization and Reform Act of 2012 (P.L. 112-95) require that the Federal Aviation Administration (FAA) take steps to accommodate routine operations of civil unmanned aircraft or drones into domestic airspace by the end of FY2015. The operation of civilian unmanned aircraft in domestic airspace raises potential security risks, including the possibility that terrorists could use a drone to carry out an attack against a ground target. It is also possible that drones themselves could be targeted by terrorists or cybercriminals seeking to tap into sensor data transmissions or to cause mayhem by hacking or jamming command and control signals.

Terrorists could potentially use drones to carry out small-scale attacks using explosives, or as platforms for chemical, biological, or radiological attacks. In September 2011, FBI disrupted a home-grown terrorist plot to attack the Pentagon and the Capitol with large model aircraft packed with high explosives.[185] The incident has raised specific concerns about potential terrorist attacks using unmanned aircraft, although the payload capacities of small unmanned aircraft would limit the damage these attacks could inflict using only conventional explosives. However, terrorists may also consider drones as a platform for carrying out a chemical, biological, or radiological attack.

In addition, routine operations of unmanned aircraft by homeland security and law enforcement agencies and others may be vulnerable to jamming or hacking that could result in a crash or hostile takeover since command and control systems typically transit over unsecured radio frequencies. Some have recommended that unmanned aircraft systems be required to have spoof-resistant[186] navigation systems and not be solely reliant on GPS guidance, since GPS signals can

[185] "Mass. Man Accused of Plotting Attack on Pentagon, Capitol," nbcnews.com, September 28, 2011. http://www.nbcnews.com/id/44705648/ns/us_news-security/#.URlBDYbDhOU.

[186] "Spoofing" is sending a counterfeit signal to a target receiver that gives unauthorized commands or false information, but appears to be from a reliable source.

be easily jammed.[187] While TSA has broad statutory authority to address a number of aviation security issues, it has not taken specific action to formally address the potential security concerns raised regarding unmanned aircraft operations in domestic airspace.

Although drones may pose security risks, they are also a potential asset for homeland security operations, particularly for CBP border surveillance operations. Law enforcement and first responders are also considering the use of drones, and their pending use raises questions regarding the potential use of DHS grants to purchase and operate drones. In addition, legal concerns, particularly Fourth Amendment and privacy concerns, regarding the law enforcement use of drones for surveillance operations have been central issues in recent public policy debate regarding drone operations in domestic airspace.

U.S. Customs and Border Protection (CBP) currently employs a fleet of 10 modified Predator B unmanned aerial vehicles (UAVs), and has ordered another 14, to augment its capabilities to patrol America's borders. Operating within specially designated airspace, these unarmed UAVs patrol the northern and southern land borders and the Gulf of Mexico to detect potential border violations and monitor suspected drug trafficking, with UAV operators cuing manned responses when appropriate. State and local governments have also expressed interest in operating UAVs for missions as diverse as traffic patrol, surveillance, and event security. Some law enforcement and first responder applications of drones may be eligible for DHS grants. A small but growing number of state and local agencies have acquired drones, some through federal grant programs, and have been issued special authorizations from FAA to fly them.[188] However, several other federal, state, and local agencies involved in law enforcement and homeland security appear to be awaiting more specific guidance from FAA regarding pending regulations covering the routine operation of drones in domestic airspace.

The introduction of drones into DHS's domestic surveillance operations presents a host of novel legal issues. Some argue that the expansion of drones into American skies may infringe upon an individual's fundamental privacy interest protected under the Fourth Amendment. To determine if certain government conduct constitutes a search or seizure under that Amendment, courts apply an array of tests (depending on the nature of the government action), including the widely used reasonable expectation of privacy test. When applying these tests to drone surveillance, a reviewing court will likely examine the location of the search, the sophistication of the technology used, and society's conception of privacy. For instance, while individuals are accorded substantial protections against warrantless government intrusions into their homes,[189] the Fourth Amendment offers fewer restrictions upon government surveillance occurring in public places,[190] and even less at the national borders.[191] Likewise, while drone surveillance

[187] Todd Humphreys, *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*, Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, July 19, 2012; U.S. Government Accountability Office, *Unmanned Aircraft Systems: Use in the National Airspace System and the Role of the Department of Homeland Security*, Statement of Gerald L. Dillingham, Ph.D., Director, Physical Infrastructure Issues, Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, July 19, 2012, GAO-12-889T.

[188] A list of organizations that applied for Certification of Authorization to operate drones is available at http://www.faa.gov/about/initiatives/uas/.

[189] See Kyllo v. United States, 533 U.S. 27 (2001).

[190] See California v. Ciraolo, 476 U.S. 207, 213 ("[W]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.") (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[191] See, e.g., United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("The Government's interest in preventing the (continued...)

conducted with relatively unsophisticated technology might be subjected to a lower level of judicial scrutiny, investigations conducted with advanced technologies such as thermal imaging or facial recognition would be submitted to closer review. Several measures have been introduced by Members of Congress that would require government agents to acquire a warrant before using drones for domestic surveillance, but would create exceptions for patrols of the national border used to prevent or deter the illegal entry of any persons or illegal substances into the United States, and for investigating credible terrorist threats.[192]

Immigration

Marc R. Rosenblum, Specialist in Immigration Policy (mrosenblum@crs.loc.gov, 7-7360)

Sources of further information, including additional CRS experts covering specific aspects of this issue, can be found in footnotes throughout this section.

Immigration policy has received substantial attention in both chambers during the 113th session of Congress.[193] In June 2013, the Senate passed the Border Security, Economic Opportunity, and Immigration Modernization Act (S. 744), a "comprehensive immigration reform" (CIR) bill that would increase immigration enforcement, require employers to use an electronic employment eligibility verification system similar to the current E-Verify program, establish three different legalization programs for unauthorized immigrants, and revise rules for both permanent and temporary immigration to the United States.[194] In the House, the Homeland Security and Judiciary Committees took action on five different bills between May and July of 2013 addressing border security, employment eligibility verification, interior immigration enforcement, and employment-based immigration.[195] This portion of the report summarizes several homeland security issues related to immigration enforcement at ports of entry and along the international border by U.S. Customs and Border Protection (CBP), the agency within DHS responsible for these activities.

Immigration Inspections at Ports of Entry

At ports of entry, CBP's Office of Field Operations (OFO) is responsible for conducting immigration, customs, and agricultural inspections of travelers seeking admission to the United States. The vast majority of people entering through U.S. ports are U.S. citizens, U.S. legal

(...continued)

entry of unwanted persons and effects is at its zenith at the international border.").

[192] H.R. 5925, S. 3287, 112th Cong. 2d Sess. (2012).

[193] For summaries of legislative activity in recent years, see CRS Report R42036, *Immigration Legislation and Issues in the 112th Congress*, coordinated by Andorra Bruno; and CRS Report R40848, *Immigration Legislation and Issues in the 111th Congress*, coordinated by Andorra Bruno.

[194] For a fuller discussion, see CRS Report R43097, *Comprehensive Immigration Reform in the 113th Congress: Major Provisions in Senate-Passed S. 744*, by Marc R. Rosenblum and Ruth Ellen Wasem.

[195] House bills receiving committee action as of August 31, 2013 include the Border Security Results Act of 2013 (H.R. 1417), the Legal Workforce Act (H.R. 1772), the Strengthen and Fortify Enforcement Act (SAFE Act, H.R. 2278), the Agricultural Guest worker Act (H.R. 1773), and the Supplying Knowledge-based Immigrants and Lifting Levels of STEM Visas Act (SKILLS Visa Act, H.R. 2131).

permanent residents (LPRs),[196] and legitimate visitors. Thus, as with cargo security (see "Cargo Security"), CBP officers' goals are to identify and intercept dangerous or unwanted (high-risk) people, while facilitating access for legitimate (low-risk) travelers. CBP seeks to accomplish these tasks without excessive infringement on privacy or civil liberties and while controlling enforcement costs.

Travelers seeking admission at ports of entry are required to present a travel document, typically a passport or its equivalent and (for non-U.S. citizens) either a visa authorizing permanent or temporary admission to the United States or proof of eligibility for admission through the Visa Waiver Program (VWP).[197] Foreign nationals are subject to security-related and other background checks prior to being issued a visa or to receiving travel authorization through the VWP. CBP officers at U.S. ports of entry verify the authenticity of travelers' documents and that each document belongs to the person seeking admission (i.e., confirm the traveler's identity). Identity confirmation relies in part on biometric checks against DHS's Automated Biometric Identification System (IDENT) database (see "Entry-Exit System"). Database interoperability allows CBP officers to check travelers' records against biographic and biometric databases managed by the Departments of Justice, State, and Defense.

The concentration of inspection activity at the border—for travelers and imports—means that sufficient resources must be present in order to minimize congestion and ensure efficient operations. CBP faces pressure to provide for the rapid processing of individuals crossing the border, but expedited processing can lead to missed opportunities for interdicting threats. Moreover, investment in ports of entry arguably has not kept pace with rapid growth in international travel and trade, and there may be inadequate infrastructure to manage flows at some ports of entry (also see "Port of Entry Infrastructure and Personnel").

In an effort to streamline admissions without compromising security, CBP has implemented several trusted traveler programs. Trusted traveler programs require applicants to clear criminal and national security background checks prior to enrollment, to participate in an in-person interview, and to submit fingerprints and other biometric data.[198] In return, trusted travelers—like trusted traders (see "Customs-Trade Partnership Against Terrorism (C-TPAT)")—are eligible for expedited processing at ports of entry. CBP currently operates three main trusted traveler programs: Global Entry, which allows expedited screening of passengers arriving at 34 major U.S. airports and 10 preclearance airports;[199] NEXUS, which is a joint U.S.-Canadian program for land, sea, and air crossings between the United States and Canada, including through dedicated vehicle lanes at 19 land ports;[200] and the Secure Electronic Network for Travelers Rapid

[196] Legal permanent residents (LPRs) are foreign nationals authorized to live lawfully and permanently within the United States; see CRS Report RL32235, *U.S. Immigration Policy on Permanent Admissions*, by Ruth Ellen Wasem.

[197] For a fuller discussion of travel requirements, see CRS Report RL31381, *U.S. Immigration Policy on Temporary Admissions*, by Ruth Ellen Wasem; CRS Report RL32235, *U.S. Immigration Policy on Permanent Admissions*, by Ruth Ellen Wasem; and CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin.

[198] Individuals are ineligible to participate in a trusted traveler program if they are inadmissible to the United States; provide false or incomplete information on trusted traveler applications; have been convicted of a criminal offense, have outstanding warrants, or are subject to an investigation; or have been found in violation of customs, immigration, or agriculture laws. Trusted travel enrollees are re-checked against certain security databases every 24 hours, every time they enter the United States, and every time they renew their trusted traveler membership. See Susan Holliday, "Global Entry Takes Off," *CBP Frontline*, Winter 2011, p. 7.

[199] CBP, "Global Entry Fact Sheet," May 2013, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/ge_factsheet_update.ctt/ge_factsheet_update.pdf.

[200] CBP, "NEXUS Fact Sheet," May 2013, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/ (continued...)

Inspection (SENTRI), which allows expedited screening at land POEs on the U.S.-Mexican border, including through dedicated vehicle lanes at 11 land ports.[201] Legislation introduced during the 113th Congress would encourage participation in trusted traveler programs by facilitating enrollment in Global Entry.[202]

Entry-Exit System

Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996 (IIRIRA, P.L. 104-208, Div. C) required the Attorney General, within two years of enactment (i.e., by September 30, 1998), to develop an automated entry and exit control system that would collect records of alien arrivals and departures and allow the Attorney General to match them in order to identify nonimmigrant aliens[203] who remain in the United States beyond the periods of their visas (i.e., visa overstayers). Congress has amended the system's requirements and deadlines on several occasions since then, including by adding a biometric component in 2001.[204] The system was initially designed primarily to identify and report on visa overstayers—thought to represent one-third to one-half of unauthorized immigrants in the United States[205]—but in the post-9/11 period it also has been seen as an important tool for identifying certain inadmissible aliens. [206]

Since 2004, the entry-exit system has been managed by the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) system, renamed the Office of Biometric Identity Management (OBIM) in March 2013.[207] US-VISIT/OBIM started at 115 airports and 14 sea ports beginning in January 2004, expanded to the 50 busiest land POEs by the end of 2004, and has been operational at almost all U.S. ports of entry since December 2006.[208]

(...continued)

nexus_facts.ctt/nexus_facts.pdf.

[201] CBP, "SENTRI Fact Sheet," May 2013, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/sentri/sentri_fact.ctt/sentri_fact.pdf.

[202] See for example, the Jobs Originated through Launching Travel Act of 2013 (H.R. 1354).

[203] Nonimmigrants are aliens admitted to the United States for a designated period of time (i.e., temporarily) and for a specific purpose; see CRS Report RL31381, *U.S. Immigration Policy on Temporary Admissions*, by Ruth Ellen Wasem.

[204] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, P.L. 107-56) §§403 and 411. Also see the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, P.L. 108-458) §7208.

[205] See CRS Report RS22446, *Nonimmigrant Overstays: Brief Synthesis of the Issue*, by Ruth Ellen Wasem.

[206] For a fuller discussion, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa Seghetti and Stephen R. Vina.

[207] The Office of Biometric Identity Management (OBIM) is a division within DHS's National Protection and Programs Directorate. The Administration's FY2014 budget request proposed (for the second year in a row) to eliminate US-VISIT/OBIM and to transfer the entry-exit program into CBP and ICE, but both chambers rejected the Administration's proposed realignment during the FY2014 cycle. See CRS Report R43147, *Department of Homeland Security: FY2014 Appropriations*, coordinated by William L. Painter.

[208] According to a 2009 GAO report, US-VISIT was operational at all 115 airports, 14 seaports, and 154 of 170 land ports. US-VISIT was not deployed to the remaining land POE's because most visitors subject to US-VISIT requirements were not authorized to use them or because, in two cases, the ports did not have the necessary transmission lines to operate US-VISIT. See U.S. Government Accountability Office, *Homeland Security: Key US-VISIT Components at Varying Stages of Completion, but Integrated and Reliable Schedule Needed*, GAO-10-13, November 2009, p. 7, http://www.gao.gov/new.items/d1013.pdf.

The system collects *biographic* entry data including names, date of birth, and travel document information from all foreign nationals entering the United States. These data are added to the Arrival and Departure Information System (ADIS) database, which included 280 million unique records as of January 2013.[209] Since 2008, ADIS also receives departure data from air carrier and sea vessel departure manifests (i.e., passenger name lists); and since September 2012 an integrated entry-exit pilot program has allowed DHS to use Canadian admissions data as U.S. departure at certain northern border land ports.[210]

OBIM and ICE compare ADIS entry and exit data to generate a list of suspected visa overstayers and to prioritize certain overstay leads for further investigation. But a July 2013 GAO report found that more than 1 million ADIS arrival records could not be matched to departure data and raised questions about the quality of DHS's overstay data.[211] Moreover, DHS and its predecessor agency have not provided Congress with statutorily required reports on visa overstays since 1994, though DHS Secretary Janet Napolitano testified in February 2013 that the department would report to Congress by the end of the year.[212] Some Members of Congress have expressed concern about visa overstays and DHS's overstay analysis;[213] and legislation being considered in the 113th Congress directs attention to visa overstays as they relate to immigration enforcement,[214] and as a metric for countries participating in the Visa Waiver Program.[215]

US-VISIT/OBIM also collects *biometric* data (i.e., fingerprints and digital photographs). Biometric data are added to the Automated Biometric Identification System (IDENT) database, which included over 150 million unique records as of January 2013.[216] But biometric data collection is more time consuming than biographic data collection, and not all travelers are required to provide biometrics. Since January 2009, US-VISIT/OBIM has collected biometric data from non-U.S. citizens entering the United States *other than* Canadian nationals admitted as

[209] US-VISIT Office of Congressional Affairs January 24, 2013.

[210] The integrated system only reports data relating to third country nationals and U.S. and Canadian permanent residents. The program operated at four ports between September 2012 and January 2013, and expanded to all automated POEs on the Canada-U.S. border beginning June 20, 2013. See Canada Border Services Agency and DHS, "Entry/Exit Information System Phase I Joint Canada-United States Report," May 8, 2013, http://www.cbsa.gc.ca/btb-pdf/eeis-ponerep-sdes-rappun-eng.html

[211] GAO, Overstay Enforcement: Additional Actions Needed to Assess DHS's Data and Improve Planning for a Biometric Air Exit Program, GAO-13-683, July 2013, http://www.gao.gov/assets/660/656316.pdf.

[212] U.S. Congress, Senate Committee on the Judiciary, *Comprehensive Immigration Reform*, testimony of DHS Secretary Janet Napolitano, 113th Cong., 1st sess., February 13, 2013.

[213] See for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Visa Security and Overstays: How Secure is America?* 113th Cong., 1st sess., May 21, 2013.

[214] For example, S. 744 would require DHS to place 90% of aliens identified as visa overstays in removal proceedings or otherwise resolve their cases.

[215] For example, the Jobs Originated through Launching Travel Act of 2013 (H.R. 1354) and the Visa Waiver Program Enhanced Security and Reform Act (H.R. 490/S. 223) would require that countries could not participate in the Visa Waiver Program if their visa overstay rate exceeds 3%.

[216] In November 2007, the IDENT database was upgraded from 2 fingerprints to 10 prints, a change that increased its accuracy for identification purposes and that allows IDENT data to be checked against the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS database includes fingerprints, criminal histories, photographs, and biographic information of more than 66 million subjects in its criminal master file along with more than 25 million sets of civil fingerprints; see Federal Bureau of Investigation, "Integrated Automated Fingerprint Identification System," http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis. IDENT/IAFIS interoperability also permits ICE automatically to check the immigration records of people booked into state and local jails through the Secure Communities program; see CRS Report R42057, *Interior Immigration Enforcement: Programs Targeting Criminal Aliens*, by Marc R. Rosenblum and William A. Kandel.

visitors, U.S. LPRs returning from cruises that begin and end in the United States or entering at land ports of entry, Mexican nationals with border crossing cards,[217] and travelers with other visas explicitly exempted from the program.[218] These exemptions meant that only about one-third of nonimmigrant admissions in FY2012 were required to provide biometric data.[219] Moreover, as of August 2013, DHS does not collect biometric departure data from any travelers leaving the United States.[220]

The completion of a more comprehensive entry-exit system has been a persistent subject of congressional concern, including in the 113th Congress. Senate-passed S. 744, for example, would require carriers to collect electronic biographic exit data (i.e., through a swiped document) from all departing air passengers, and would make the implementation of this electronic exit system one of the "triggers" for the complete implementation of the bill's legalization provisions for certain unauthorized immigrants.[221] The bill also would require DHS, within two years of enactment, to establish a *biometric* exit system at the ten U.S. airports with the greatest volume of international air travel.[222] The House-reported Border Security Results Act of 2013 (H.R. 1417) would require DHS, within 180 days, to submit a plan to Congress either to immediately complete a biometric entry-exit system, or to implement an alternative program within two years.

Enforcement Between Ports of Entry

> For more information, see CRS Report R42138, *Border Security: Immigration Enforcement Between Ports of Entry*.

Between ports of entry, CBP's U.S. Border Patrol (USBP) is responsible for enforcing U.S. immigration law and other federal laws along the border and for preventing all unlawful entries into the United States, including entries of terrorists, unauthorized aliens, instruments of terrorism, narcotics, and other contraband. In the course of discharging its duties, the Border Patrol patrols 7,494 miles of U.S. international borders with Mexico and Canada and the coastal

[217] Border crossing cards (BCC, also known as "laser visas") are short-term multiple-entry, 10-year nonimmigrant visas that may be issued to certain citizens of Mexico for business or tourism. BCC holders are permitted to visit the United States for up to 30 days and must remain within a zone up to 25 miles from the border in Texas, New Mexico, and California or within 75 miles of the border in Arizona.

[218] U.S. Department of Homeland Security, Privacy Impact Assessment Update for the United States Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT) in Conjunction with the Final Rule (73 FR 7743), Enrollment of Additional Alien in US-VISIT," February 10, 2009, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addl%20aliens.pdf.

[219] According to DHS data, there were about 165 million nonimmigrant admissions to the United States in FY2012, including about 54 million (33%) I-94 admissions (generally subject to US-VISIT) and about 106 million tourists and business travelers from Canada and Mexicans with BCCs; see Randall Monger, *Nonimmigrant Admissions to the United States: 2012*, U.S. Department of Homeland Security Office of Immigration Statistics, Annual Flow Report, August 2103, http://www.dhs.gov/sites/default/files/publications/ois_ni_fr_2012.pdf.

[220] US-VISIT tested a pair of pilot programs in 2009 to collect biometric data from departing air passengers and a pilot program in 2009-2010 to collect biometric data from departing temporary workers at a pair of land ports in Arizona, but did not view either program as viable and scalable models for biometric exit data collection. See U.S. Government Accountability Office, *Homeland Security: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options*, GAO-10-860, August 2010, p. 4, http://www.gao.gov/new.items/d10860.pdf; and DHS, *Comprehensive Biometric Air Exit Plan: Fiscal Year 2012 Report to Congress*, May 11, 2012.

[221] For a fuller discussion, see CRS Report R43097, *Comprehensive Immigration Reform in the 113th Congress: Major Provisions in Senate-Passed S. 744*, by Marc R. Rosenblum and Ruth Ellen Wasem.

[222] Ibid.

waters around Florida and Puerto Rico. Debate during the 113th Congress has focused on what additional investments are needed to secure the border and on metrics for measuring border security.

With support from Congress, DHS and its predecessor agency the Immigration and Naturalization Service (INS) have invested in border security personnel, fencing and infrastructure, and surveillance technology since the 1980s, with CBP's budget totaling $11.8 billion in FY2013.[223] The Senate CIR bill S. 744 would expand these investments, doubling the number of Border Patrol agents assigned to the southern border and requiring DHS to install at least 700 miles of pedestrian fencing. The bill would pay for these new border assets with about $45 billion in direct spending over a 5-10 year period.[224]

Some Members of Congress have raised questions about whether DHS's investments at the border have been effective, and some have argued that enforcement has been compromised by the fact that DHS does not have a single, overarching strategy for border security.[225] Congress also has raised questions about how to measure border security. The Border Patrol traditionally has used border apprehensions as its primary measure of border security, and these apprehensions have fallen sharply since 2006.[226] Yet falling apprehensions may reflect the downturn in U.S. labor markets and/or a change in tactics by unauthorized migrants, among other variables, in addition to enforcement. Thus, apprehensions are an imprecise indicator of the effectiveness of border enforcement.

Bills in both chambers would require DHS to report to Congress on a strategy to secure U.S. borders and to develop more precise metrics of border security. In the House, H.R. 1417 would require DHS to develop a comprehensive strategy to gain and maintain "operational control" of the border within deadlines established by the bill. The bill defines metrics for such control, and would require DHS to collaborate with outside partners and with the Government Accountability Office (GAO) to develop, review, and report on these metrics. The Senate CIR bill, S. 744, also would require DHS to submit a pair of new border strategies, with the contents of the Senate bill's strategies defined to encompass the new border enforcement resources required by the bill.

[223] By comparison, the enforcement-related budget of the legacy Immigration and Naturalization Service was $380 million in 1986, according to CRS calculations from U.S. Office of Management and Budget, *Budget of the U.S. Government: Appendix*, Washington, DC, 1987 For a fuller discussion of FY2014 appropriations, see CRS Report R43147, *Department of Homeland Security: FY2014 Appropriations*, coordinated by William L. Painter.

[224] The deployment of these new border assets would be one of several "triggers" for the implementation of legalization provisions in S. 744. For a fuller discussion, see CRS Report R43097, *Comprehensive Immigration Reform in the 113th Congress: Major Provisions in Senate-Passed S. 744*, by Marc R. Rosenblum and Ruth Ellen Wasem.

[225] See for example, U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *A Study in Contrasts: House and Senate Approaches to Border Security*, 113th Cong., 1st sess., July 23, 2013. The Border Patrol published a national strategy for controlling U.S. borders in May 2012, building on three earlier strategies published between 1994 and 2005. The new strategy describes USBP's approach to risk management and to striking a balance among its traditional emphasis on preventing illegal migration and its post-9/11 priority missions of preventing the entry of terrorists and terrorist weapons, along with the recent U.S. focus on combating transnational criminal organizations. But the strategy does not describe operational plans or address the interaction among the Border Patrol and other federal agencies (including other parts of DHS) with responsibilities at the border.

[226] The border patrol reported 327,577 alien apprehensions along the Southwest border in FY2011, the lowest number since FY1972; see U.S. Border Patrol, Total Illegal Alien Apprehensions By Fiscal Year, http://www.cbp.gov/linkhandler/cgov/border_security/border_patrol/usbp_statistics/60_10_app_stats.ctt/60_11_app_stats.pdf.

Congress may also question the relative priority attached to the southern and northern borders. While the Southwest border has experienced more unauthorized immigration, some security experts have warned that the northern border may represent a more important point of vulnerability when it comes to terrorism and related threats to homeland security—especially in light of the more limited enforcement resources deployed there.[227]

CBP Integrity

An additional issue of possible concern to Congress is the integrity of CBP agents and others involved with security at and between U.S. ports of entry. CBP places a great amount of responsibility upon its inspection officers, and smugglers and other nefarious actors have attempted—sometimes successfully—to infiltrate CBP. Moreover, criminals have reportedly made extensive efforts to surreptitiously enroll CBP officers on their payrolls, particularly in the wake of drug supply chain interruptions by the ongoing Mexican drug-related violence and the tactical measures implemented by DHS. To counteract such efforts, DHS has ramped up its internal investigation efforts to root out any double agents. These integrity programs have been accompanied by increased professionalization measures, such as the addition of law enforcement retirement benefits for CBP officers that incentivize employees to resist corruption. Congress appropriated $10 million in emergency supplemental funding in FY2010 to support these integrity efforts (P.L. 111-230) and held hearings on the subject during the 112th Congress.[228] A December 2012 GAO report found that CBP had not completed an integrity strategy, and that it faced challenges in managing and overseeing integrity-related programs.[229] An August 2013 GAO report found that CBP's integrity strategy was still being drafted, but that the agency's integrity-related training courses were "systematic and integrated."[230] Congress may continue to monitor CBP integrity issues.

[227] See, e.g., U.S. Government Accountability Office, *Border Security: Enhanced DHS Oversight and Assessment of Interagency Cooridination is Needed for the Northern Border*, GAO-11-97, December 2010, http://www.gao.gov/new.items/d1197.pdf. Also see CRS Report R42969, *Border Security: Understanding Threats at U.S. Borders*, by Marc R. Rosenblum, Jerome P. Bjelopera, and Kristin Finklea.

[228] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Ad Hoc Subcommittee on Disaster Recovery, *Border Corruption: Assessing Customs and Border Protection and the Department of Homeland Security Inspector General's Office Collaboration in the Fight to Prevent Corruption*, 112th Cong., 1st sess., June 9, 2011.

[229] GAO, *Border Security: Additional Actions Needed to Strengthen CBP Efforts to Mitigate Risk of Employee Corruption and Misconduct*, GAO-13-59, December 4, 2012.

[230] GAO, *U.S. Customs and Border Protection Provides Integrity-Related Training to Its Officers and Agents throughout Their Careers*, GAO-13-769R, August 28, 2013.

Disaster Preparedness, Response, and Recovery

Disaster Assistance Funding

Bruce R. Lindsay, Analyst in American National Government (blindsay@crs.loc.gov, 7-3752)

The majority of disaster assistance provided by the Federal Emergency Management Agency (FEMA) to states and localities after a declared emergency or major disaster is funded with monies from the Disaster Relief Fund (DRF).[231]

In general, Congress annually appropriates budget authority to the DRF to ensure that funding is available for recovery projects from previous incidents (some of these projects take several years to complete) and to create a reserve to pay for emergencies and major disasters that might occur that fiscal year. Any remaining balance in the DRF at the end of the fiscal year is carried over to the next fiscal year.[232] However, in some cases—particularly in recent years—there have been shortfalls in the DRF. In such cases, additional budget authority has typically been provided through a continuing resolution or an emergency supplemental appropriation. The additional funding traditionally has either been designated as an emergency requirement or as disaster relief under the Budget Control Act, designations that allow funding beyond the limitations of the discretionary budget limits.

From FY2005 to FY2010, Congress provided additional budget authority for the DRF through a combination of supplemental and continuing appropriations nine times. The reliance on emergency supplemental appropriations has been of particular congressional concern. Supplemental appropriations legislation usually carries an emergency designation for its funding, and therefore are not subject to the limits opposed by discretionary spending allocations. However, the number of disasters being declared over the last two decades has risen, as have their costs.[233] These upward trends have led some to discuss how to reduce and/or offset federal spending on major disasters.

Partly in response to these discussions, Congress included provisions on disaster relief spending when it passed P.L. 112-25, the Budget Control Act (BCA).[234] The BCA sets overall discretionary spending caps and provides two types of adjustments that could be applied to make room for disaster assistance—a limited adjustment specifically for the costs of major disasters under the Stafford Act, and an unlimited adjustment for more broadly defined emergency spending.[235] The

[231] For further analysis on emergency and major disaster declarations see CRS Report RL34146, *FEMA's Disaster Declaration Process: A Primer*, by Francis X. McCarthy.

[232] The methodology used to determine the initial request by the Administration for the DRF incorporates four data points. These points include (1) the available appropriation, (2) the DRF monthly average (the amount in the DRF), (3) the monthly cost estimates for catastrophic events, and (4) the estimated monthly recoveries of unobligated funds. Disasters costing $500 million or more have been considered outliers and are not factored in the calculation.

[233] For further analysis on Stafford Act declarations from 1953 to 2011 see CRS Report R42702, *Stafford Act Declarations 1953-2011: Trends and Analyses, and Implications for Congress*, by Bruce R. Lindsay and Francis X. McCarthy.

[234] For further analysis on disaster assistance under the Budget Control Act see CRS Report R42352, *An Examination of Federal Disaster Relief Under the Budget Control Act*, by Bruce R. Lindsay, William L. Painter, and Francis X. McCarthy.

[235] The Office of Management and Budget (OMB) manages the sequestration process and the limits on adjustments (continued...)

adjustment limitation is not a restriction on disaster assistance—it is a restriction on how much the discretionary budget cap can be adjusted upward to accommodate the assistance.

FY2013 represented the first fiscal year in which the DRF received all of the funding available under the BCA's allowable adjustment for disaster relief, and the first time that disaster relief in excess of the allowable adjustment was covered by an emergency designation. The DRF had roughly $7.3 billion available for disaster needs when Hurricane Sandy made landfall in the northeastern United States in October 2012. The anticipated demand on the DRF was high enough, however, that Congress approved $11.49 billion in additional pre-sequester resources for the DRF the following January through P.L. 113-2, the Disaster Relief Appropriations Act, 2013. The total FY2013 funding requested for major disasters under the Stafford Act would have exceeded the available allowable adjustment of $11.78 billion—even before accounting for the other disaster assistance requested by the Administration.[236] The Administration sought, and Congress provided, emergency funding designations to cover most of the supplemental funding that exceeded the allowable adjustment. Of the $11.49 billion provided for the DRF in P.L. 113-2, $5.38 billion used the allowable adjustment for disaster relief under the BCA, and $6.11 billion carried an emergency designation.[237]

However, there were attempts in Congress to offset the costs of the disaster relief. Amendments were offered in both the House and the Senate to offset the disaster package—including the funding for the DRF. H.Amdt. 4 (which would have offset $17 billion in the immediate disaster assistance with an across-the-board cut in discretionary spending) was not agreed to by a vote of 162-258.[238] S.Amdt. 4 (which would have offset the entire $51 billion in disaster assistance) was not agreed to by a vote of 35-62.[239]

Disaster relief funding generally remained subject to the impact of sequestration. Of the $17.89 billion provided to the DRF in FY2013, $898 million was cancelled by sequestration.

In response to concerns over the increasing federal expenditures on disaster relief, Congress may consider passing reforms to reduce these expenditures, or implement other measures to address their impact on the national debt. Some examples include changing emergency and major disaster declaration criteria to limit the number of events eligible for federal assistance, and reducing the standard 75% federal to state cost-share for recovery to a lower percentage (such as 50%).

(...continued)

available to raise the spending cap. The BCA requires OMB to annually calculate the adjusted 10-year rolling average of disaster relief spending that sets the allowable cap adjustment for disaster relief.

[236] The allowable adjustment for disaster assistance for FY2013 was $11.8 billion, $6.4 billion of which was already available to the DRF under the terms of P.L. 112-175. The Administration's request for assistance in the immediate wake of the storm was $60.7 billion.

[237] P.L. 113-2, Title X, Chapter 6.

[238] Roll No.14, January 15, 2013.

[239] Record Vote Number 3, January 28, 2013.

Hurricane Sandy Recovery

Jared T. Brown, Analyst in Emergency Management and Homeland Security Policy (jbrown@crs.loc.gov, 7-4918)

For more information, see CRS Report R42869, *FY2013 Supplemental Funding for Disaster Relief*, and CRS Report R42991, *Analysis of the Sandy Recovery Improvement Act of 2013*.

On the evening of October 29, 2012, Hurricane Sandy, the second-largest Atlantic storm on record, made landfall in southern New Jersey. The consequences of the storm were considered to be immense: at least 159 people died, over 23,000 people required temporary shelters, 8.5 million customers were left without power, approximately $65 billion in damages, and 650,000 homes damaged or destroyed.[240] As with other catastrophic natural disasters, Members of Congress responded to Hurricane Sandy by holding a series of hearings to gather information,[241] visiting the affected region for a firsthand assessment of the damage and to confer with state and local officials, and introducing and acting on legislation based on that process. As a result of the storm, the President declared major disasters for 12 states as well as the District of Columbia under the authority of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act, P.L. 93-288 as amended).[242]

On January 29, 2013, the Disaster Relief Appropriations Act, 2013, a $50.5 billion package of disaster assistance largely focused on responding to Hurricane Sandy, was enacted as P.L. 113-2. In addition, Congress provided an additional $9.7 billion in borrowing authority for the National Flood Insurance Program (NFIP) as P.L. 113-1 on January 6, 2013. The Disaster Relief Appropriations Act, 2013 provided supplemental funding to over 66 different accounts and programs, including $16.0 billion for the Community Development Block Grant (CDBG) program, $11.5 billion for the Disaster Relief Fund, $10.9 billion for the Public Transportation Emergency Relief Program, and $5.4 billion total for disaster-related activities of the U.S. Army Corps of Engineers.[243]

[240] Extensive descriptions of the Hurricane Sandy storm and its impacts can be found in Hurricane Sandy Rebuilding Task Force, *Hurricane Sandy Rebuilding Strategy: Stronger Communities, a Resilient Region*, Washington, DC, August 2013, pp. 18-22, at http://portal.hud.gov/hudportal/documents/huddoc?id=HSRebuildingStrategy.pdf; and at Federal Emergency Management Agency, *Hurricane Sandy FEMA After-Action Report*, Washington, DC, July 1, 2013, p. 7, at http://www.fema.gov/media-library/assets/documents/33772.

[241] See, for example, House Committee on Transportation and Infrastructure, *A Review of the Preparedness, Response to and Recovery from Hurricane Sandy*, 112th Cong., 2nd sess., December 4, 2012, and Senate Committee on Appropriations, Subcommittee on Homeland Security Appropriations, *Hurricane Sandy: Response and Recovery - Progress and Challenges*, 112th Cong., 2nd sess., December 5, 2012.

[242] The Stafford Act is codified at 42 U.S.C. 5121 et seq. The major disaster declarations are: New York (DR-4085); New Jersey (DR-4086); Connecticut (DR-4087); Rhode Island (DR-4089); Delaware (DR-4090); Maryland (DR-4091); Virginia (DR-4092); West Virginia (DR-4093); New Hampshire (DR-4095); the District of Columbia (DR-4096); Massachusetts (DR-4097); Ohio (DR-4098); and Pennsylvania (DR-4099). More information on each declaration is available at http://www.fema.gov/disasters.

[243] On March 1, 2013, as required pursuant to Sec. 251A of the Balanced Budget and Emergency Deficit Control Act, the Administration ordered an automatic across-the-board cancellation of budget authority, known as sequestration. This resulted in a $2.5 billion reduction in the budget authority provided by the Disaster Relief Appropriations Act, leaving $48.0 billion available for use. A full breakdown of the supplemental funding, as enacted by Congress, and how it compares to the Administration's request submitted on December 7, 2012, is available in Table 1 of the CRS Report R42869, *FY2013 Supplemental Funding for Disaster Relief*, coordinated by William L. Painter and Jared T. Brown.

In addition to evaluating the need for supplemental appropriations in response to Hurricane Sandy, the 112th and 113th Congresses considered reforming provisions of the Stafford Act. Generally, concerns were raised that the recovery from Hurricane Sandy would be plagued by perceived delays and bureaucratic burdens that inhibited the recovery following Hurricane Katrina. The Sandy Recovery Improvement Act of 2013 (SRIA), passed as Division B of P.L. 113-2, the Disaster Relief Appropriations Act, 2013, revised the Stafford Act in response to these concerns as well as other considerations.[244]

In recognition of the scale and complexity of Hurricane Sandy, the Administration initiated a coordinated effort across multiple federal agencies to support the region in responding to and recovering from the disaster. On December 7, 2013, President Barack Obama issued Executive Order (E.O.) 13632, *Establishing the Hurricane Sandy Rebuilding Task Force*.[245] The Task Force was intended to coordinate federal interagency efforts to provide for an efficient recovery process. Chaired by the Secretary of Housing and Urban Development, Shaun L. S. Donovan, the Task Force included members from 27 different executive branch agencies and White House offices.[246] The Task Force was supported by an advisory group composed of many state, tribal, and local elected leaders from the most severely impacted cities and towns in the region, mainly from New York and New Jersey.[247]

The key deliverable of the Task Force, as mandated by Section 5 of E.O. 13632, is the Hurricane Sandy Rebuilding Strategy (HSRS). The HSRS is a wide-ranging, lengthy policy document providing 69 different recommendations for a long-term recovery plan for the impacted region across eight major topic areas, entitled:

- Promoting Resilient Rebuilding Through Innovative Ideas and a Thorough Understanding of Current and Future Risk;
- Ensuring a Regionally Coordinated, Resilient Approach to Infrastructure Investment;
- Restoring and Strengthening Homes and Providing Families with Safe, Affordable Housing Options;
- Supporting Small Businesses and Revitalizing Local Economies;
- Addressing Insurance Challenges, Understanding, and Affordability;
- Building State and Local Capacity to Plan for and Implement Long-Term Recovery and Rebuilding;
- Improving Data Sharing Between Federal, State, and Local Officials; and
- Data Sharing Between Federal Agencies and State and Local Governments.

[244] For a detailed review of SRIA, Division B of P.L. 113-2, please see CRS Report R42991, *Analysis of the Sandy Recovery Improvement Act of 2013*, by Jared T. Brown, Francis X. McCarthy, and Edward C. Liu.

[245] Executive Order 13632, "Establishing the Hurricane Sandy Rebuilding Task Force," 77 *Federal Register* 74341, December 14, 2012.

[246] For membership details, see Hurricane Sandy Rebuilding Task Force, *Hurricane Sandy Rebuilding Strategy: Stronger Communities, a Resilient Region*, Washington, DC, August 2013, pp. 196-198, at http://portal.hud.gov/hudportal/documents/huddoc?id=HSRebuildingStrategy.pdf. Henceforth referred to as the HSRS in footnotes.

[247] HSRS, pp. 8-9.

In their totality, the recommendations of HSRS represent a strategic vision by the Administration for the Hurricane Sandy recovery process, including how federal funds should be expended, how federal agencies should synchronize their efforts, and how the region can leverage the recovery process from Sandy to prepare for future disasters.

There are numerous issues that may arise in the 113th Congress in relation to the recovery process for Hurricane Sandy. For example, the HSRS includes many recommendations that would require further action by the executive branch to apply them to the greater benefit in future disasters. Though each recommendation is subject to unique challenges, in general, effective implementation will require a coordinated regulatory and policy-review process among numerous federal agencies. Several other recommendations would require legislative amendments to apply them both for Hurricane Sandy and for other disasters. Therefore, the 113th Congress may wish to continue its oversight of the Sandy recovery process with an appreciation for its impact on the nation's future disaster recovery capacity. Understandably, the impacted region itself continues to face many known and unknown future challenges in their recovery from the storm. The 113th Congress may also wish to continue its oversight of the expenditure and use of supplemental appropriations in the affected region to improve the delivery of federal assistance in addressing these anticipated challenges.

DHS State and Local Preparedness Grants

Natalie Keegan, Analyst in American Federalism and Emergency Management Policy (nkeegan@crs.loc.gov, 7-9569)

State and local governments have primary responsibility for most domestic public safety functions. When facing difficult fiscal conditions, state and local governments may reduce their level of contribution towards public safety and, consequently, homeland security preparedness, due to increasing pressure to address tight budgetary constraints and fund competing priorities. Since state and local governments fund the largest percentage of public safety expenditures, this may have a significant impact on the national preparedness level. On March 30, 2011, President Obama issued a presidential policy directive that directed the Secretary of DHS to develop and submit to the President a national preparedness goal. The DHS Secretary released the National Preparedness Goal in September 2011:

> A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.[248]

One means of implementing the National Preparedness Goal is to link grant funded activities to the Goal. Prior to 9/11, there were only three federal grant programs available to state and local governments to address homeland security: the State Domestic Preparedness Program administered by the Department of Justice, the Emergency Management Performance Grant (EMPG) administered by the Federal Emergency Management Agency (FEMA), and the Metropolitan Medical Response System (MMRS) administered by the Department of Health and Human Services. Since that time, several additional homeland security grant programs were added to ensure state and local preparedness, including the State Homeland Security Grant

[248] U.S. Department of Homeland Security webpage, at http://www.fema.gov/preparedness-1/national-preparedness-goal, accessed on January 10, 2013.

Program (SHSGP), Citizen Corps Program (CCP), Urban Area Security Initiative (UASI), Driver's License Security Grants Program (REAL ID), Operation Stonegarden grant program (Stonegarden), Regional Catastrophic Preparedness Grant Program (RCPG), Public Transportation Security Assistance and Rail Security Assistance grant program (Transit Grants), Port Security Grants (Port Security), Over-the-Road Bus Security Assistance (Over-the-Road), Buffer Zone Protection Program (BZPP), Interoperable Emergency Communications Grant Program (IECGP), and Emergency Operations Center Grant Program (EOC).

While state and local governments receive federal assistance for preparedness activities, this federal assistance accounts for only a small percentage of overall state and local spending for public safety. On average, total expenditures for all state and local governments for public safety is $218 billion annually.[249] Public safety expenditures include costs associated with the functions of police protection, fire protection, correction, and protective inspections and regulations.[250] In FY2010, Congress appropriated approximately $4.1 billion to federal grant programs for state and local government homeland security preparedness.[251] In FY2011, Congress appropriated approximately $3.3 billion to federal grant programs for state and local government homeland security preparedness. For FY2012, Congress appropriated $2.3 billion in federal grants for state and local government homeland security preparedness.[252] In FY2013, Congress provided 1.5 billion for state and local programs.[253] These amounts account for less than 2% of state and local government public safety costs. Since state and local governments are critical in the overall preparedness efforts of the nation, Congress may wish to review how to best provide assistance to ensure appropriate levels of state and local preparedness in the changing fiscal conditions facing the nation.

Consolidation of DHS State and Local Programs

In FY2013, the President requested $1.8 billion in federal grants for state and local government homeland security preparedness. The requested funding level included funding to support the establishment of a National Preparedness Grant Program (NPGP), which was proposed as a means to consolidate the activities previously funded under a number of state and local preparedness grant programs. Congress did not provide funding or authorization for NPGP in FY2013. In FY2014, the Administration repeated this approach by requesting $1.1 billion for the National Preparedness Grant Program.

Congressional justification for denying the FY2013 preparedness grant consolidation included concern over the lack of congressional authorization for the NPGP and lack of clarity in how the program would be implemented. In its report on FY2013 funding recommendations for DHS, the House Appropriations Committee denied a request by the Administration to consolidate several state and local preparedness grant program activities under a National Preparedness Grant Program because it had not been authorized by Congress, lacked sufficient details regarding the implementation of the program, and lacked sufficient stakeholder participation in the

[249] U.S. Census Bureau, *State and Local Government Finance Summary Report*, April 2011, p. 7.

[250] The definition of state and local public safety expenditures is based on the U.S Census Bureau's definition of public safety for the annual surveys of state and local government finances.

[251] This amount includes appropriations for the Firefighters Assistance Grants.

[252] P.L. 112-74, Consolidated Appropriations Act, 2012. This amount includes funding for Firefighter Assistance Grants and Emergency Management Performance Grant.

[253] P.L. 113-6.This amount is after the across-the-board cuts but prior to applying sequestration.

development of the proposal.[254] The Senate Appropriations Committee also expressed concern with the proposal to consolidate the state and local preparedness grants because it was unclear how risk assessments would be used and how funding would be allocated.[255] The Senate Committee also noted its concern over the uncertainty surrounding the allocation of funding to individual grant programs.[256] While the FY2014 proposal by the administration provided additional detail regarding the structure of the proposed NPGP, Congress continues to express concern regarding the program authorization and implementation.[257] The 113th Congress could continue to debate authorization, appropriations, and structure for DHS preparedness grants.

Firefighter Assistance Programs

Lennard G. Kruger, Specialist in Science and Technology Policy (7-7070, lkruger@crs.loc.gov)

For further information, see CRS Report RL32341, *Assistance to Firefighters Program: Distribution of Fire Grant Funding* and CRS Report RL33375, *Staffing for Adequate Fire and Emergency Response: The SAFER Grant Program.*

While firefighting activities are traditionally the responsibility of states and local communities, Congress has established federal firefighter assistance grant programs within DHS to provide additional support for local fire departments. In 2000, the 106th Congress established the Assistance to Firefighters Grant Program (AFG), which provides grants to local fire departments for firefighting equipment and training. In the wake of the 9/11 attacks, the scope and funding for AFG were subsequently expanded. Additionally in 2003, the 108th Congress established the Staffing for Adequate Fire and Emergency Response (SAFER) program, which provides grants to support firefighter staffing.

In the 113th Congress, debate over firefighter assistance programs is likely to take place within the appropriations process. Arriving at funding levels for AFG and SAFER is subject to two countervailing considerations. On the one hand, inadequate state and local public safety budgets have led many to argue for the necessity of maintaining, if not increasing, federal grant support for fire departments. On the other hand, concerns over reducing overall federal discretionary spending have led others to question whether continued or reduced federal support for AFG and SAFER is warranted.

Meanwhile, the 112th Congress reauthorized AFG and SAFER in the FY2013 National Defense Authorization Act (P.L. 112-239). The reauthorized statute makes changes in AFG grant caps and distribution formulas, and removes or changes certain SAFER grant restrictions and limitations. The 113th Congress will likely oversee the impact of AFG and SAFER grant changes mandated by the reauthorization. The continuing issue is how effectively grants are being distributed and used to protect the health and safety of the public and firefighting personnel against fire and fire-related hazards.

[254] P.L. 112-74, Consolidated Appropriations Act, 2012. This amount includes funding for Firefighter Assistance Grants and Emergency Management Performance Grant.

[255] S.Rept. 112-169, p. 113.

[256] Ibid.

[257] H.Rept. 113-91, p. 94. S.Rept. 113-77, p. 117.

Emergency Communications Infrastructure and Technology

Linda K. Moore, Specialist in Telecommunications Policy (lmoore@crs.loc.gov, 7-5853)

Emergency communications systems support first responders and other emergency personnel, disseminate alerts and warnings to residents in endangered areas, and relay calls for help through 911 call networks. Their networks support day-to-day needs to protect the safety of the public and deliver critical information before, during, and after disasters.

The technologies that support emergency communications are converging toward a common platform using the Internet Protocol (IP). Federal, state, and local agencies are investing in IP-enabled communications infrastructure that can be shared to support all forms of emergency communications. Notable examples of new investment are (1) interoperable public safety communications networks; (2) digital alerts and warnings; and (3) Next-Generation 9-1-1 (NG9-1-1) networks.

Notable federal programs, in addition to grant programs, are the First Responder Network Authority (FirstNet); the Integrated Public Alert and Warning System (IPAWS); and the 9-1-1 Implementation Coordination Office (ICO). FirstNet is an independent authority established within the National Telecommunications and Information Administration (NTIA). IPAWS is coordinated through the National Continuity Programs Directorate of the Federal Emergency Management Agency with the participation of the Federal Communications Commission. The functions of ICO are shared by the NTIA and the National Highway Traffic Safety Administration. None of the enacted legislation that guides these programs requires coordination of planning and investment among them. FirstNet is required to share infrastructure where technically and economically feasible and to provide connectivity to 9-1-1 call centers, but its charter is limited to developing a new wireless network for emergency personnel.

FirstNet was created and ICO reauthorized by the Middle Class Tax Relief and Job Creation Act of 2012,[258] Title VI. The act requires both entities to submit periodic reports to Congress. In addition to these oversight responsibilities, the 113th Congress is likely to consider legislation to improve IPAWS, as several bills for this purpose were introduced in the 112th. The survivability, availability, and coverage of commercial communications infrastructure are concerns that are likely to be considered in tandem with emergency communications policies. Commercial telecommunications lines and switches, wireless infrastructure, and radio and television broadcasting facilities are examples of critical components where failure can jeopardize public safety. Multiple federal agencies and congressional committee jurisdictions, as well as state, local, and tribal authorities, have responsibility for different components. While the National Response Framework addresses coordination of response operations efforts across jurisdictions, there is no federal policy that recognizes the need to coordinate technology procurement decisions and infrastructure investments for emergency communications. The transition to IP-based communications provides the opportunity to identify and coordinate infrastructure investments.

[258] P.L. 112-96.

Presidential Policy Directive 8 and the National Preparedness System

Jared T. Brown, Analyst in Emergency Management and Homeland Security Policy
(jbrown@crs.loc.gov, 7-4918)

The United States is threatened by a wide array of hazards, including natural disasters, acts of terrorism, viral pandemics, and manmade disasters such as the *Deepwater Horizon* oil spill. The way the nation strategically prioritizes and allocates resources to prepare for disasters can significantly influence the ultimate cost to society, both in the number of human casualties and the scope of economic damage. Presidential Policy Directive 8: National Preparedness (PPD-8), signed and released by President Barack Obama on March 30, 2011, and its component policies intend to guide how the nation, from the federal level to private citizens, can "prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation."[259] These threats include terrorist acts, natural disasters, and other man-made incidents. PPD-8 evolves from, and supersedes, Homeland Security Presidential Directive 8, which was released under President George W. Bush.[260] PPD-8 is intended to meet many requirements of Subtitle C of the Post-Katrina Emergency Reform Act of 2006 (P.L. 109-295, 6 U.S.C. §741-764).

PPD-8 is not a stand-alone document. To date, it is supported by the issuance of a National Preparedness Goal, a report on the National Preparedness System, and the 2012 and 2013 National Preparedness Reports.[261] Additionally, there are four finalized National Planning Frameworks that formulate strategic guidance in each of the mission areas of prevention, mitigation, response, and recovery.[262] A National Protection Framework remains in draft as of September 17, 2013. There are also additional elements of the National Preparedness System that will help operationalize the policy guidance of PPD-8.[263]

In brief, PPD-8 and its many component policies embody the strategic vision and planning of the federal government as it relates to preparing the nation for disasters. PPD-8 sets the goal for how "prepared" the nation should be to prevent, protect, mitigate, respond to, and recover from disasters, and establishes a general framework and roadmap achieving that level of preparedness. In this respect, PPD-8's influence is theoretically similar to the National Security Strategy's influence on military preparedness and foreign affairs in terms of its strategic purpose and

[259] White House, *Presidential Policy Directive 8: National Preparedness*, Washington, DC, March 30, 2011, p. 1, http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

[260] White House, *Homeland Security Policy Directive 8: National Preparedness*, Washington, DC, December 17, 2003. http://www.dhs.gov/files/publications/gc_1189788256647.shtm.

[261] For the 2012 preparedness report, see Department of Homeland Security, *National Preparedness Report*, Washington, DC, March 30, 2012, at http://www.fema.gov/media-library/assets/documents/26675?id=5914. For the 2013 preparedness report, see Department of Homeland Security, *National Preparedness Report*, Washington, DC, March 30, 2012,at http://www.fema.gov/media-library/assets/documents/32509?id=7465.

[262] For copies of the National Prevention Framework, National Mitigation Framework, National Response Framework 2.0, the National Disaster Recovery Framework, and other documents related to the National Preparedness System, see FEMA's "National Preparedness Resource Library" at http://www.fema.gov/national-preparedness-resource-library.

[263] For example, PPD-8 calls for a Campaign to Build and Sustain Preparedness, a National Training and Education System, a National Exercise Program, and a Remedial Action Management Program. These components are also mandated, in various formats, in statute.

potential impact on budgetary decision-making, the assignment of national roles and responsibilities, and long-term policy objectives for disaster preparedness. The *actual* impact of PPD-8 is yet to be determined and will be difficult to assess, though it will be determined in large part by:

- The quality of the strategic planning and the clarity of the resulting guidance, especially as it relates to the assignment of national roles and responsibilities and the analysis of core capabilities in the National Planning Frameworks and in the Federal Interagency Operations Plans.
- The acceptance of and adherence to the strategic guidance provided in PPD-8 by national stakeholders, especially state, tribal, and local governments and their respective emergency management agencies.
- The way that PPD-8 policies inform the budgetary planning process by the Administration, the appropriations process by Congress, and the budget/appropriations processes of state and local governments, especially as it relates to the prioritization of limited resources to provide homeland security and emergency management core capabilities.

The 113th Congress may wish to continue its oversight of how the Administration implements PPD-8 and manages the National Preparedness System writ large on the above factors and more, such as:

- evaluating how PPD-8 policies conform to the intentions of the PKEMRA statute;
- how federal roles and responsibilities have been assigned to implement and execute PPD-8 policies; and
- how non-federal resources and stakeholders will be impacted by national preparedness guidance.

Public Health and Medical Services

Sarah A. Lister, Specialist in Public Health and Epidemiology (slister@crs.loc.gov, 7-7320)

The nation's public health emergency management laws expanded considerably in the past decade, reflecting lessons from the terrorist attacks in 2001 and Hurricane Katrina in 2005, in particular. Incidents since then—the H1N1 influenza pandemic in 2009; the earthquake in Haiti and the *Deepwater Horizon* oil spill in 2010; nuclear plant failures following an earthquake and tsunami in Japan in 2011; and Hurricane Sandy in 2012—each revealed persistent gaps in the nation's readiness for public health and medical emergencies. These gaps include existing response plans may not sufficiently anticipate situations that arise; the technology needed to assess threats (such as radiation or chemical exposure) may be limited; medical countermeasures (i.e., vaccines, antidotes, or treatments for harmful exposures) may not be available in adequate amounts, if at all; the means to distribute existing countermeasures in a timely manner may be limited; the medical system lacks sufficient capacity to provide care in response to a mass casualty incident; and funding for response costs may not be immediately available, if at all. Given the robust roles of the private sector and state and local governments in preparedness and response efforts, the federal government's ability to affect these efforts through funding and other policies may also be limited.

The 113th Congress reauthorized the body of law that directs most public health and medical preparedness and response activities in the Department of Health and Human Services (HHS), through the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013 (PAHPRA, P.L. 113-5). The reauthorization focused in particular on improving federal programs to assure the availability of medical countermeasures in an emergency.[264] PAHPRA also reauthorized grants to states for public health and health system preparedness, as well as funding for a number of other specific programs. In general, the appropriations amounts that are authorized for programs under PAHPRA are lower than the amounts authorized for the same programs in the 2006 reauthorization.[265] Finally, PAHPRA required the establishment of a National Advisory Committee on Children and Disasters. This Committee has not yet been established.

Funding for the response to a public health incident is a challenge when the incident does not lead to a declaration under the Stafford Act.[266] The HHS Secretary has authority for a no-year Public Health Emergency Fund, but Congress has not appropriated monies to the fund for many years.[267] Assistance under the Stafford Act can help federal, state, and local agencies with the costs of public health activities such as assuring food and water safety, and monitoring illness rates in affected communities. However, there is no federal assistance program designed specifically to cover the uninsured or uncompensated costs of individual health care—including mental health care—that may be needed as a consequence of a disaster. (There is no consensus that this should be a federal responsibility.) Nonetheless, when faced with mass casualty incidents, hospitals, physicians, and other providers may face considerable pressure to deliver care without a clear source of reimbursement. On several occasions, Congress has provided special assistance to address uncompensated disaster-related health care costs after an incident.[268] The Patient Protection and Affordable Care Act (ACA, P.L. 111-148, as amended) may mitigate future concerns about disaster-related health care costs by decreasing the ranks of the uninsured.[269]

Potential Reauthorization of the Defense Production Act of 1950

Jared T. Brown, Analyst in Emergency Management and Homeland Security Policy (jbrown@crs.loc.gov, 7-4918)

For more information, see CRS Report R43118, *The Defense Production Act of 1950: History, Authorities, and Reauthorization*.

[264] See for example FDA, "About the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013 (PAHPRA)," http://www.fda.gov/emergencypreparedness/medicalcountermeasures/ucm346195.htm.

[265] P.L. 109-417, the Pandemic and All-Hazards Preparedness Act. Actual appropriations for most of these programs have also decreased since 2006.

[266] The Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288, as amended. See CRS Report RL34724, *Would an Influenza Pandemic Qualify as a Major Disaster Under the Stafford Act?*, by Edward C. Liu; and CRS Report RL33053, *Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding*, by Francis X. McCarthy.

[267] CRS Report RL33579, *The Public Health and Medical Response to Disasters: Federal Authority and Funding*, by Sarah A. Lister.

[268] CRS Report RL33927, *Selected Federal Compensation Programs for Physical Injury or Death*, coordinated by Sarah A. Lister and Charles S. Redhead; GAO, *Hurricane Katrina: Allocation and Use of $2 Billion for Medicaid and Other Health Care Needs*, GAO-07-67, February 28, 2007, http://www.gao.gov; CRS Report R40554, *The 2009 Influenza Pandemic: An Overview*, by Sarah A. Lister and Charles S. Redhead; and CRS Report R41232, *FY2010 Supplemental for Wars, Disaster Assistance, Haiti Relief, and Other Programs*, coordinated by Amy Belasco.

[269] CRS reports on ACA implementation are available at http://www.crs.gov/pages/subissue.aspx?cliid=3746.

The Defense Production Act of 1950, as amended (DPA, 50 U.S.C. Appx. §§2061 *et seq.*), provides the President an "array of authorities to shape national defense preparedness programs and to take appropriate steps to maintain and enhance the domestic industrial base."[270] The term *national defense*, as defined in the statute, guides the potential use of the authorities of the DPA and includes activities relating to homeland security.[271] Though DPA authorities are most frequently used by the Department of Defense to enhance U.S. military preparedness and capabilities, DPA authorities can be, and have been, used to support domestic homeland security activities and the nation's preparedness for, response to, and recovery from natural disasters, terrorist attacks, and other national emergencies. For example, DPA authorities have been used to support the Federal Bureau of Investigation's Terrorist Screening Center program and the U.S. Army Corp of Engineers' Greater New Orleans Hurricane and Storm Damage Risk Reduction System program, and to enable the private sector's restoration of rail service following Hurricane Katrina.[272]

The President is granted a wide range of authorities in the DPA. In brief, authorities in Title I of the DPA allow the President to issue priority contracts for critical materials, equipment, and services produced in the private market. Persons receiving these priority contracts are required to fulfill them before any other non-prioritized competing private or government obligation, thereby ensuring that the government has timely access to these goods in the interest of national defense. Authorities in Title III of the DPA allow the government to incentivize and expand the domestic productive capacity and supply of critical equipment, technologies, and resources vital to the national defense. Title VII of the DPA includes a number of provisions, including the authority to establish voluntary agreements within the private sector in the interest of national defense,[273] and authorities that support the activities of the Committee on Foreign Investment in the United States (CFIUS).[274] In the statute, almost all authorities of the DPA are granted to the President. The President, in turn, has delegated many of these authorities to subordinates by issuing executive orders. Most recently, the President issued Executive Order 13603 on "National Defense Resources Preparedness" primarily to establish policies for using DPA authorities and to delegate the authorities to Cabinet Secretaries in the executive branch.[275]

Most DPA authorities are not permanently authorized. Rather, they are time-limited, undergoing periodic amendment and reauthorization. In 2009, Congress amended the DPA and reauthorized the majority of its provisions. That reauthorization is set to expire on September 30, 2014.[276] Therefore, the 113th Congress may consider reauthorizing and amending the DPA before it

[270] 50 U.S.C. Appx. §2062(a)(4); §2(a)(4) of the DPA.

[271] For the definition of national defense in the DPA, see 50 U.S.C. Appx. §2152(14); §702(14) of the DPA.

[272] For more examples of how DPA authorities have been and can be used to support homeland security activities, see Department of Homeland Security, *The Defense Production Act Committee: Report to Congress*, Washington, DC, August 2011, p. 8; or Department of Homeland Security, *Use of the Defense Production Act to Reduce Interruptions in Critical Infrastructure and Key Resource Operations During Emergencies*, April 25, 2008, pp. 18-19; or The National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies: Final Report and Recommendations*, Appendix G: The Defense Production Act, Washington, DC, July 14, 2009, p. 48.

[273] 50 U.S.C. Appx. §2158; §708 of the DPA. This provision offers parties to such agreements limited protection from antitrust statutes.

[274] 50 U.S.C. Appx. §2170, §721 of the DPA. For more on CFIUS, see CRS Report RL33388, *The Committee on Foreign Investment in the United States (CFIUS)*, by James K. Jackson.

[275] Executive Order 13603, 77 Fed. Reg. 16651 (Mar. 22, 2012).

[276] See P.L. 111-67 for the last reauthorization of the DPA.

expires.[277] Committees in both chambers of the 113th Congress have held hearings on potential reauthorization.[278] Additionally, Congress may wish to review its oversight of the current use of DPA authorities by federal agencies, especially as it relates to the creation of regulations for Title I authorities and the ongoing activities of the Defense Production Act Committee.[279]

Management Issues at DHS

DHS Reorganization Authority

Henry B. Hogue, Analyst in American National Government (hhogue@crs.loc.gov, 7-0642)

From the establishment of the Department of Homeland Security (DHS) in January 2003 through 2007, the President and the Secretary of Homeland Security used provisions of the Homeland Security Act of 2002, most notably Section 872,[280] to implement a number of major and minor departmental reorganizations. Some reorganization activities under these authorities were carried out in conjunction with the implementation of the Post-Katrina Emergency Management Reform Act of 2006.[281]

Since May 2007, Congress has limited the use of appropriated funds for carrying out Section 872 reorganizations. Section 3501 of the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007, enacted on May 25, 2007, instituted such limitations for the balance of FY2007, stating:

> None of the funds provided in this Act, or P.L. 109-295 [Department of Homeland Security Appropriations Act, 2007], shall be available to carry out section 872 of P.L. 107-296 [Homeland Security Act of 2002].[282]

Succeeding DHS appropriations acts up through and including that for FY2013 included similar provisions.[283]

[277] Several reauthorization bills in the past have only extended the sunset date, with no major revisions to the DPA, while others have amended the authorities while also extending the expiration date.

[278] See U.S. Congress, House Committee on Financial Services, Subcommittee on Monetary Policy and Trade, *Reauthorizing the Defense Production Act*, 113th Cong., 1st sess., May 8, 2013, H. Hrg. 113-8 (Washington: GPO, 2013); and U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, *Oversight of the Defense Production Act: Issues and Opportunities for Reauthorization*, 113th Cong., 1st sess., July 16, 2013 (pre-published).

[279] The Defense Production Act Committee (DPAC) is a new interagency body established by the 2009 reauthorization of the DPA to advise the President regarding the effective use of authorities granted to the President by the DPA and delegated by E.O. 13603. The DPAC website is at http://www.dpacommittee.com/dpac.htm.

[280] P.L. 107-296; 116 Stat. 2135 at 2243.

[281] Implementation of certain provisions of the Post-Katrina Emergency Management Reform Act of 2006 was interwoven into a January 2007 reorganization under the Secretary's authority.

[282] P.L. 110-28; 121 Stat. 112 at 143.

[283] See, for example, a provision of the Consolidated Appropriations Act, 2008: "None of the funds provided in this Act shall be available to carry out section 872 of Public Law 107–296" (P.L. 110-161, §546; 121 Stat. 2080). Similar provisions were included in the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329, §529; 122 Stat. 3686); the Department of Homeland Security Appropriations Act, 2010 (P.L. 111-83, §525; 123 Stat. 2173); the Consolidated Appropriations Act, 2012 (P.L. 112-74, Division D, §523; 125 Stat. 974); and (continued...)

The scope and effect of this limitation were the subject of a July 2008 Government Accountability Office (GAO) opinion.[284] This opinion raised the question of whether a reorganization could be undertaken under authorities that, absent Section 872, might be available to the Secretary. These include the authorities identified by the department: implied authority to organize and manage the department;[285] redelegation authority; and authority under 5 U.S.C. Section 301, which authorizes an agency head to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property."

Since the appropriations acts are annual, the decision of whether or not to carry over the limitation arises each year. More broadly, the question of whether and how Section 872 might be amended may be at issue as part of a reauthorization process. Such decisions might hinge, in part, on a congressional determination of the impact of Section 872 and the appropriation limitation on the management and functioning of the department.

The Management Budget

William L. Painter, Analyst in Emergency Management and Homeland Security Policy (wpainter@crs.loc.gov, 7-3335)

For more information, see CRS Report R42644, *Department of Homeland Security: FY2013 Appropriations.*

Title I of the Homeland Security Appropriations bill contains the funding for the primary management functions of DHS. Originally envisioned as a skeleton staff, the headquarters and management functions have grown in response to criticism of the department's ability to effectively oversee its own activities. In debates over departmental funding, questioning the size and effectiveness of the department's management cadre is a common theme.

In FY2003, the first year of DHS operations, $195 million was provided for management accounts. In FY2012, those accounts were funded at $803 million. This growth is due to several factors, including increases in staff size required to perform oversight functions, rising personnel costs, technology investments, and increasing real estate expenses for the department's headquarters offices. In recent years, these accounts have been requested at higher levels than might otherwise be expected due to the inclusion of significant capital initiatives, such as

(...continued)

the Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6, Division D, Sec. 522; 127 Stat.371). The final continuing resolution for FY2011 appears to have carried the FY2010 provision forward for the fiscal year ending September 30, 2011. See P.L. 112-10, the Department of Defense and Full-Year Continuing Appropriations Act, 2011; 125 Stat. 38. §1104 of the act provides that, "Except as otherwise expressly provided in this division, the requirements, authorities, conditions, limitations, and other provisions of the appropriations Acts referred to in section 1101(a) shall continue in effect through the date specified in section 1106 [September 30,2011]" (125 Stat. 103). The Department of Homeland Security Appropriations Act, 2010 (P.L. 111-83), which contains the limitation provision, is among those referred to in §1101(a).

[284] U.S. Government Accountability Office, *Department of Homeland Security—Transfer of Support Function for Principal Federal Officials*, B-316533, July 31, 2008, http://www.gao.gov/decisions/appro/316533.pdf. Hereafter, B-316533.

[285] See Basil J. Mezines, Jacob A. Stein, and Jules Gruff, *Administrative Law*, vol. 1 (New York: Matthew Bender, 2006), pp. 4-18 to 4-27.

headquarters consolidation and data center migration in these accounts, and personnel initiatives aimed at boosting the department's cadre of acquisition oversight staff and reducing the number of contractors in sensitive positions.

Pre-sequester, these accounts received $643 million in FY2013. The Administration requested funding for the management accounts for FY2014 at $651 million, not including $106 million for headquarters consolidation or $54 million for data center consolidation. House and Senate Appropriations Committees recommended $526 million and $633 million, respectively, for the management accounts with similar exclusions. House amendments reduced the funding in the bill by $51 million from the committee's recommendation, and $176 million below the Administration's requested level.

DHS Financial Management Reforms

Natalie M. Keegan, Analyst in American Federalism and Emergency Management Policy (nkeegan@crs.loc.gov, 7-9569), and William L. Painter, Analyst in Emergency Management and Homeland Security Policy (wpainter@crs.loc.gov, 7-3335)

From its inception, DHS has faced financial management challenges. Transferring components and their budgets between agencies is a complex process in the best of situations, but doing it in the process of establishing a new department that is performing important national security missions from its first day of operations adds additional complexity. This was further compounded by inherited financial management problems that existed at several major legacy components, including the Coast Guard, FEMA, and elements that formed ICE.[286]

The department tried to develop its own financial management system in-house through a project known as "eMerge2," but failed. A second attempt was made to implement a department-wide system through contracting with outside developers under the Transformation and Systems Consolidation initiative, or TASC. After GAO ruled that DHS had improperly awarded the initial $450 million contract—the latest result from a series of protests and legal challenges that had delayed the project—the award was cancelled and the project shelved.[287]

Although the department has been on the GAO High Risk List since it was created, progress has been made on reducing the number of material weaknesses in the department's financial controls. FY2012 was the first year since its establishment that DHS was able to complete an audit of all its financial statements. KMPG, the independent auditor, said that DHS was unable to represent that property, plant, and equipment (PP&E) balances were correct in its financial statements or provide adequate evidence to support the balances included. Nevertheless, the DHS OIG considers even a qualified audit "a significant milestone."[288]

[286] For examples of DHS program management and financial management issues, see U.S. Department of Homeland Security, Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, OIG-13-09, November 2012; U.S. Government Accountability Office, *Managing Preparedness Grants and Assessing National Capabilities: Continuing Challenge Impede FEMA's Progress*, GAO-12-526T, March 20, 2012; U.S. Department of Homeland Security, Office of Inspector General, *FEMA's Efforts to Recoup Improper Payments in Accordance with the Disaster Assistance Recoupment Fairness Act of 2011*, OIG-12-127, September 2012.

[287] House Committee on Government Oversight and Reform, Subcommittee on Government Organization, Efficiency and Financial Management, "Department of Homeland Security Financial Management," May 13, 2011. Documents available at http://oversight.house.gov/hearing/financial-management-at-the-department-of-homeland-security/.

[288] Office of Inspector General, Department of Homeland Security, OIG-13-20, "Independent Auditors' Report on (continued...)

The independent auditor noted five deficiencies in internal controls[289] that were significant enough to be considered material weaknesses:

- Financial Reporting;
- Information Technology Controls and Financial System Functionality;
- Property, Plant and Equipment;
- Environmental and Other Liabilities; and
- Budgetary Accounting.

While all five of these material weaknesses persisted from FY2011 to FY2012, the DHS OIG noted significant progress with the Coast Guard's ability to account for its PP&E—an important step, as the Coast Guard has roughly half of DHS's PP&E.[290]

GAO noted the following in its audit of the government's FY2011 and FY2012 consolidated financial statements:

> It is important that DHS continue to remediate its internal control deficiencies and build on the progress it has made as it moves forward to achieve its ultimate goal of obtaining clean audit opinions on its fiscal year 2013 financial statements and on its internal control over financial reporting.[291]

The 113th Congress will likely continue its interest in DHS's efforts to improve its internal financial systems, given the relative size of the department's budget, the interest expressed in this issue by authorizing committee leadership, and the current drive for stricter budgetary oversight.

These issues could be examined at the department, component, or program level. Oversight might include a review of the internal financial and administrative controls in the administration of specific grant programs, and improper payments made under the programs. Consideration of the internal financial and management controls might include the extent to which DHS is complying with existing control standards, penalties for noncompliance, and whether the standards should be adjusted to account for any unique elements in the DHS programs.

(...continued)

DHS' FY2012 Financial Statements and Internal Control over Financial Reporting," November 2012, p. 1.

[289] Internal control standards seek to ensure that the use of funds comply with applicable laws, that assets are appropriately protected against waste, fraud, and abuse, and that federal agencies have efficient and effective financial and program administration systems that allow for appropriate accountability of funds. Internal control standards are integrated into program management protocols, including quarterly program and financial monitoring, timely submission of single audit reports and grants closeout, and improper payments testing and reporting.

[290] Office of Inspector General, Department of Homeland Security, OIG-13-09, :"Major Management Challenges Facing the Department of Homeland Security," December 2012, p. 22.

[291] Dodaro, Gene L., Comptroller General of the United States, transmittal letter accompanying GAO-13-271R "Financial Audit: U.S. Government's Fiscal Years 2012 and 2011 Consolidated Financial Statements," January 17, 2013, p. 3.

Headquarters Consolidation

William L. Painter, Analyst in Emergency Management and Homeland Security Policy (wpainter@crs.loc.gov, 7-3335)

For additional information, see CRS Report R42753, *DHS Headquarters Consolidation Project: Issues for Congress*.

The Department of Homeland Security's headquarters footprint occupies more than 7 million square feet of office space in about 50 separate locations in the greater Washington, DC, area. This is largely a legacy of how the department was assembled in a short period of time from 22 separate federal agencies which were themselves spread across the National Capital region. The fragmentation of headquarters is cited by the department as a major contributor to inefficiencies, including time lost shuttling staff between headquarters elements; additional security, real estate, and administrative costs; and reduced cohesion among the components that make up the department.

To unify the department's headquarters functions, the department approved a $3.4 billion master plan to create a new DHS headquarters on the grounds of St. Elizabeth's in Anacostia. According to GSA, this is the largest federal office construction since the Pentagon was built during World War II. $1.4 billion of this project was to be funded through the DHS budget, and $2 billion through the GSA.[292] Thus far $460 million has been appropriated to DHS for the project and $908 million to GSA through FY2013. Phase 1A of the project—a new Coast Guard headquarters facility—has been completed with the funding already provided by Congress and is now in use.

In 2013, a revised construction schedule was developed, projecting lower levels of appropriations and a longer timeline for the project. Under the new projection, the project would be completed in FY2026 at a cost $4.5 billion.[293] According to GSA, even with the cost increases from delaying funding, the project would still result in over $530 million in projected savings compared to leasing over the next 30 years. This estimate does not take into account the costs GSA would have to incur to stabilize and maintain the St. Elizabeths campus if the project were halted, or the efficiencies for DHS that a consolidate headquarters would generate.[294]

With headquarters consolidation remaining a priority for the Administration, the Coast Guard moving into its new facility on the campus, and current budgetary constraints altering both the growth projections that were the basis for DHS's consolidation plans and the prospects for funding in coming fiscal years, legislative action in the 113th Congress could help clarify the future for this project.

[292] U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *Homeland Security Headquarters Facilities*, 111th Cong., 2nd sess., March 25, 2010 (Washington: GPO, 2010), pp. 335-366.

[293] "St. Elizabeths Development Revised Baseline," document provided by DHS, June 12, 2013.

[294] "Prospectus—Construction: Department of Homeland Security Consolidation at St. Elizabeths, Washington DC," PDC-0002-WA14, p. 14. As downloaded from GSA.gov.

Department of Homeland Security Personnel Issues

Barbara L. Schwemle, Analyst in American National Government (bschwemle@crs.loc.gov, 7-8655).

For more information, see the section on Departmental Management in CRS Report R43147, *Department of Homeland Security: FY2014 Appropriations*.

An essential consideration underlying the mission and performance of the Department of Homeland Security (DHS) is human resource management (HRM). Responsibility for HRM is vested in the Office of the Chief Human Capital Officer (OCHCO), an entity organizationally and for appropriations purposes located within the Under Secretary for Management. The OCHCO plays a critical role in supporting and executing the department's "Strategic Plan for Fiscal Years 2012-2016."[295] The current chief human capital officer assumed the position on August 4, 2011, and with the change in the appointment from political to career status, is the first career member of the Senior Executive Service to hold the office. During the 113th Congress, the House of Representatives and the Senate may conduct oversight of personnel issues at the department. Among the issues that have persisted since the establishment of DHS are those related to the recruitment and hiring of highly qualified candidates, diversity of the workforce, and employee morale. Current initiatives in each of these areas are discussed below.

Recruitment and Hiring of Highly Qualified Candidates

DHS has struggled to develop and maintain a highly skilled workforce in a number of areas, including cybersecurity. In a report published in fall 2012, the Cyberskills Task Force of the Homeland Security Advisory Council[296] recommended that the department build a team of employees, numbering some 600, with cybersecurity skills that are critical to the DHS mission. The task force also recommended that a pilot DHS Cyber Reserve Program be established to make certain that "DHS cyber alumni and other talented cybersecurity experts outside of government are known and available to DHS in times of need."[297] The Secretary of Homeland Security accepted the task force recommendations.[298] In an opinion piece published in April 2013, she said that the department is:

- "creating and implementing standards of performance through a professional certification system,"

[295] U.S. Department of Homeland Security, *Strategic Plan FY 2012-2016* (Washington, DC: 2012), pp. 25-26, available at http://www.dhs.gov/xlibrary/assets/dhs-strategic-plan-fy-2012-2016.pdf. Hereafter referred to as DHS, Strategic Plan.

[296] The Homeland Security Academic Advisory Council provides advice and recommendations to DHS on matters related to, among other issues, student and recent graduate recruitment; homeland security academic programs; and cybersecurity. The department is the lead agency for the Cybersecurity Workforce Structure component of the National Initiative for Cybersecurity Education whose goal is "to establish an operational, sustainable and continually improving cybersecurity education program for the nation." See, http://www.dhs.gov/homeland-security-academic-advisory-council-hsaac and http://csrc.nist.gov/nice/workforce.htm.

[297] U.S. Department of Homeland Security, Homeland Security Advisory Council, *Cyberskills Task Force Report*, (Washington: Fall 2012), available at https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

[298] Nicole Johnson, "DHS to Hire 600 Cyber Professionals," *Federal Times*, FedLine, October 31, 2012.

- "creating a standardized and comprehensive training and development program to grow and retain our existing cybersecurity workforce,"
- "establishing a dynamic Cyber Surge Capacity Force composed of certified cybersecurity professionals with critical skills in the private sector, who will be readily available for rapid support and deployment,"
- and "extending the scope of cyber education beyond the federal workplace ... to include the public, as well as students from kindergarten through post-graduate school."[299]

DHS has requested legislative authority that would permit it to expedite the hiring process for and provide higher rates of compensation to cyber-skilled employees. Currently pending in the 113th Congress is legislation that would authorize the department to establish cybersecurity positions in the excepted service, directly appoint candidates to positions, and provide compensation and benefits beyond what Title 5, United States Code would authorize.[300]

In the absence of legislative action, DHS has launched a number of initiatives to help develop the workforce it needs, including in cybersecurity.

On October 24, 2012, the Homeland Security Secretary announced the establishment of a Secretary's Honors Program (SHP) "to recruit exceptional recent graduates for careers" in DHS.[301] Under the program, individuals with relevant graduate, undergraduate, or law degrees may apply for one-year or two-year fellowships in information technology, cybersecurity, policy, management, emergency management, and law. Individuals selected for the program will participate in rotations throughout DHS, be mentored, receive training, and participate in programs for professional development. Upon successful completion of the program, participants may be converted to permanent employees within the department.[302]

On February 22, 2013, DHS launched the National Initiative for Cybersecurity Careers and Studies (NICCS), an online resource for cybersecurity career, education, and training information. The initiative was developed through the close partnership of DHS, the National Institute of Standards and Technology, the Office of the Director of National Intelligence, the Department of

[299] Janet Napolitano, "Cyber Education Key to Security," *Politico*, April 8, 2013, available at http://www.politico.com/story/2013/04/cyber-education-key-to-security-89715.html. Additional information is provided in Department of Homeland Security, *Congressional Budget Justification FY2014* (Washington: DHS, April 2013), references to the cybersecurity workforce are at pp. 34, 2518, 2570, 2629-2630, and 3440 of the electronic document, available at http://www.dhs.gov/dhs-budget.

[300] Representative Michael McCaul introduced H.R. 756, the Cybersecurity Enhancement Act of 2013, which passed the House of Representatives on a roll call vote (No. 107) of 402-16 on April 16, 2013. Senator John Rockefeller introduced S. 1353, the Cybersecurity Act of 2013, which was ordered to be reported by the Senate Committee on Commerce, Science, and Transportation on July 30, 2013. The provision on Federal Cyber Scholarship for Service is at Section 106(e) of the House bill and Section 302(e) of the Senate bill.

[301] U.S. Department of Homeland Security, "Secretary Napolitano Announces Employment Honors Program at Academic Advisory Council Meeting," news release, October 24, 2012, available at http://www.dhs.gov/news/2012/10/24/secretary-napolitano-announces-employment-honors-program.

302 U.S. Department of Homeland Security, "Secretary's Honors Program," available at https://www.dhs.gov/secretarys-honors-program. In remarks at the Center for Strategic and International Studies on October 25, 2012, Secretary Napolitano said that the program is designed for 50 fellows who "will be given special mentorships, special projects, really see the upper reaches of the department in terms of leadership," available at http://search.proquest.com/docview/1115140892?accountid=12084.

Defense, the Department of Education, the National Science Foundation, and the Office of Personnel Management. It combines government, industry, and academia efforts to "provide a comprehensive, single resource to address the nation's cybersecurity knowledge needs."[303]

In April 2013, the department began the SHP Cyber Student Initiative, "to engage exceptional community college students" in working at a U.S. Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI) forensics lab. The initiative offers "unpaid student volunteer positions to current two-year community college students and student veterans pursuing a program of study in a cybersecurity-related field."[304]

Diversity of the Workforce

The department's strategic plan stated an objective of "pursu[ing] greater diversity in the workforce, especially at senior levels."[305] Other than specifying that a senior-level steering committee, chaired by the Deputy Secretary of DHS, will "direct a sustained effort to improve diversity," the plan did not provide any details on the initiative. Data reported by the Office of Personnel Management (OPM) provide some insight on the department's workforce characteristics. As of March 2013 (most current data available) the on-board civilian workforce at DHS numbered 196,799. Of this total, 82,468, or 41.9%, were classified as minority. Among ethnicity and racial groups represented in the department's workforce were American Indian or Alaskan Native (1,306, or 0.7% of the total), Asian (8,947, or 4.5% of the total), Black/African American (29,467, or almost 15.0% of the total), Native Hawaiian/Pacific Islander (871, or 0.4% of the total), and Hispanic/Latino (23,901, or 12.1% of the total).[306] OPM also reported that DHS had 24 employees on the senior-level (SL) pay schedule, and 610 employees on the Senior Executive Service (SES) pay schedule. None of the SL employees were classified as minority. The SES total included 122, or 20% minority, of which none were American Indian or Alaskan Native, or Native Hawaiian/Pacific Islander; 13, or 2.1%, were Asian; 59, or 9.7%, were Black/African American; and 29, or 4.7%, were Hispanic/Latino.[307]

Women employed by DHS numbered 65,147, or 33% of the department's workforce total. (OPM's database does not provide data on gender by ethnicity and race.) Six women were paid on the SL pay schedule (25% of the SL total) and 173 (28.4% of the SES total) are paid on the

[303] U.S. Department of Homeland Security, "DHS Launches National Initiative for Cybersecurity Careers and Studies," news release, February 21, 2013, available at http://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies. The NICCS website is available at http://niccs.us-cert.gov/.

[304] U.S. Department of Homeland Security, "DHS Announces Cyber Student Initiative," news release, April 18, 2013, available at http://www.dhs.gov/news/2013/04/18/dhs-announces-cyber-student-initiative, and "DHS Secretary's Honors Program Cyber Student Initiative," available at http://www.dhs.gov/sites/default/files/publications/SHP_Cyber_Student_Initiative_Bulletin.pdf.

[305] DHS, Strategic Plan, p. 26.

[306] U.S. Office of Personnel Management, FedScope Database, diversity cubes, available at http://www.fedscope.opm.gov/employment.asp. The Office of Personnel Management defines on-board employment as the number of employees in pay status at the end of the quarter (or end of the pay period prior to the end of the quarter). Comparing the March 2013 data with that as of March 2012 shows that total employment decreased by 1,007, or -0.5% and minority employment increased by 959, or 1.2%. Employment of American Indians or Alaskan Natives decreased by 66, or -4.8%; Asians increased by 220, or 2.5%; Blacks/African Americans increased by 207, or 0.7%; Native Hawaiians/Pacific Islanders increased by 64, or 7.9%; and Hispanics decreased by 764, or -3.1%.

[307] Comparing the March 2013 data with that as of March 2012 shows that the number of SL employees increased by 4, or 20% and the number of SES employees increased by 3, or 0.5%. The number of SES employees who were Asian remained the same; Black/African American increased by 2, or 3.5%; and Hispanic/Latino increased by 1, or 3.3%.

SES pay schedule.[308] The strategic plan stated that DHS would institute an exit survey department-wide to provide information on employee attrition and its impact on the diversity of the workforce, but information on the department's procedures are not publicly available. The DHS website lists several reports related to diversity in the department.[309] In June 2013, the Secretary stated that the department had prepared its first Diversity and Inclusion Strategic Plan, but further information about the plan was not provided.

Employee Morale

Testifying before a March 22, 2012, hearing conducted by the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, the department's CHCO, Catherine Emerson, stated that a concerted effort, characterized by "improved employee communication, training, emphasis on diversity and inclusion, and employee recognition," and strengthened leadership by managers and supervisors, was underway to improve morale among DHS employees.[310] Particular steps to carry out the initiative were not provided. Results from the annual Federal Employee Viewpoint Survey conducted by OPM have consistently found low morale at DHS. The most recent survey results, released by OPM on November 21, 2012,[311] again reported a decline in the department's ratings. In the ranking of agencies represented in the survey, according to four key indices, DHS placed low, and even lower than its relative positions in the 2011 survey. Specifically, the department's ranks (out of 37 agencies) and overall scores for the 2012 survey, as compared with the 2011 survey, were as follows: Leadership and Knowledge Management—36/52 (33/55 in 2011), Results-Oriented Performance Culture—36/46 (35/48 in 2011), Talent Management—35/50 (33/53 in 2011), and Job Satisfaction—35/61 (33/64 in 2011).[312] A May 2013 report from the Partnership for Public Service that was based on the results of the Employee Viewpoint Survey ranked DHS in last place among seventeen other large agencies in terms of innovation. The report gave the department an innovation score of 52.7%, a decline of -2.6% over the previous year. Among the 292 agency subcomponents that were ranked in the report, the United States Coast Guard was the highest

[308] Ibid. FedScope database, employment cubes. Comparing the March 2013 data with that as of March 2012 shows that the number of women increased by 129, or 0.2%, women on the SL pay schedule remained the same and women on the SES pay schedule decreased by 7, or -3.9%.

[309] U.S. Department of Homeland Security, "EEO and Diversity Reports and Resources," available at http://www.dhs.gov/eeo-and-diversity-reports-and-resources.

[310] Written testimony of DHS Chief Human Capital Officer Catherine Emerson for a House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management hearing titled "Building One DHS: Why is Employee Morale Low?," March 22, 2012, available at http://www.dhs.gov/news/2012/03/22/written-testimony-dhs-chief-human-capital-officer-house-homeland-security.

[311] U.S. Office of Personnel Management, 2012 Federal Employee Viewpoint Survey Results, available at http://www.fedview.opm.gov/2012/. In the Department of Homeland Security, 82,218 employees responded to the survey for a participation rate of 46.5%.

[312] U.S. Office of Personnel Management, 2012 Federal Employee Viewpoint Survey Results, Agency Rankings, available at http://www.fedview.opm.gov/2012/Ranking/. The Leadership and Knowledge Management Index measures the extent to which employees hold their leadership in high regard. The Results-Oriented Performance Culture Index measures the extent to which employees believe their organizational culture promotes improvement in processes, products, and services, and organizational outcomes. The Talent Management Index measures the extent to which employees think their organization has the talent necessary to achieve its organizational goals. The Job Satisfaction Index measures the extent to which employees are satisfied with their jobs and various aspects of their jobs.

placed DHS component with a rank of 74 and an innovation score of 67.2%, an increase of 0.8% over the previous year.[313]

Congress could mandate that the Department of Homeland Security provide periodic updates, during hearings on the budget request and other matters, on the progress of its initiatives to address each of these issues. For example, the House Committee on Appropriations, in its report accompanying the FY2014 Department of Homeland Security Appropriations bill, directed the department to report to the relevant committees of jurisdiction on a corrective action plan to address concerns about morale and innovation.[314]

In addition, review and evaluation of the OCHCO by Congress on a regular basis throughout the year could continue to inform legislative oversight of current and developing HRM policies at DHS. The chief human capital officer also could be directed to provide detailed information on the OCHCO webpage that would be updated at designated intervals and include copies of specific plans (such as the Diversity and Inclusion Strategic Plan) to fulfill the department's HRM initiatives (such as those related to the recruitment and hiring, diversity, and employee morale issues) and advances in accomplishing them. For oversight purposes, Congress may be interested in examining the department's procedures for exit interviews,[315] the findings of the interviews, and any procedures established by DHS to consider the results.

Acquisition

L. Elaine Halchin, Specialist in American National Government (ehalchin@crs.loc.gov, 7-0646)

The Department of Homeland Security ranked sixth among federal agencies in procurement spending in FY2012. In constant dollars (2012), DHS spent $4.8 billion in FY2003 and $12.4 billion in FY2012.[316] During this same time period, government-wide procurement spending increased from $381.7 billion (2012 constant dollars) to $514.4 billion.

Acquisition Workforce

As the Services Acquisition Reform Act (SARA) Panel noted in its 2007 report, the federal acquisition workforce has "shortcomings in terms of size, skills, and experience,"[317] and DHS is

[313] Partnership for Public Service, *Best Places to Work in the Federal Government Analysis Most Innovative Agencies* (Washington: Partnership, May 2013), pp. 1, 5, 9, available at http://ourpublicservice.org/OPS/publications/viewcontentdetails.php?id=222. The report defines innovation as "the process of improving, adapting or developing a product, system or service to deliver better results and create value for people."

[314] U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *Department of Homeland Security Appropriations Bill, 2014*, report to accompany H.R. 2217, 113th Congress, 1st sess., H.Rept. 113-91 (Washington: GPO, May 29, 2013), p. 14, available at http://www.gpo.gov/fdsys/pkg/CRPT-113hrpt91/pdf/CRPT-113hrpt91.pdf.

[315] A post on the Careers blog of the *Wall Street Journal* commented on increasing the usefulness of such exit interviews or conversations and stated that, "By finding out what spurred valued staffers to look elsewhere, managers can get to the real reasons employees feel disengaged or unhappy." Lauren Weber, "The One Question to Ask in an Exit Interview," *Wall Street Journal*, February 21, 2013, available at http://blogs.wsj.com/atwork/2013/02/21/the-one-question-to-ask-in-an-exit-interview/.

[316] Using data obtained from USASpending.gov, CRS calculated FY2010 constant dollars.

[317] U.S. Government Accountability Office, Department of Homeland Security: A Strategic Approach Is Needed to (continued...)

no exception. In 2008, GAO reported that the department did not have "adequate staff to effectively plan and execute contracts."[318] In the same report, GAO acknowledged that "DHS's initiatives are positive steps toward building an effective acquisition workforce," but also noted that the department needs to engage in long-term strategic workforce planning.[319]

Potentially positive steps include the department's development and implementation of a Procurement Staffing Model and a strategic plan for its acquisition function, which includes several acquisition workforce initiatives. DHS reported in June 2012 that it was implementing the staffing model, which was designed to provide "optimal numbers" of personnel needed to award and administer contracts.[320] Additionally, the Chief Procurement Officer's (CPO's) strategic plan for FY2012-FY2014 includes the following acquisition workforce initiatives: "continue [the] acquisition professional career program ... improve [the] quality of [the] contracting workforce ... and promote employee retention."[321] Responsible officials and performance metrics are identified for each initiative.

Balanced Workforce Strategy (BWS)

In early 2009, DHS announced that, as part of its efficiency review, department components would examine how to achieve a proper balance between federal employees and contractor employees. The strategy has three goals:

- Complying with applicable statutes, regulations, and policies, through a repeatable, documented decision-making process;
- Determining the proper balance of federal and contractor employees for programs and functions; and
- Reducing mission risk, while as practicable, reducing or controlling cost.[322]

The department's BWS process involves identifying and analyzing the work (e.g., the statement of work (SOW) included in a service contract), and implementing the sourcing decision that results from the analysis.[323] The department's Balanced Workforce Program Management Office, and an affiliated departmental working group, lead the effort and provide oversight.

The topics discussed here suggest several questions that may be of interest to the 113rd Congress. Regarding the department's acquisition workforce, does the department have sufficient funding to

(...continued)

Better Ensure the Acquisition Workforce Can Meet Mission Needs, GAO-09-30, November 19, 2008, p. 5, at http://www.gao.gov/new.items/d0930.pdf.

[318] Ibid., p. 2.

[319] Ibid., pp. 27-28.

[320] U.S. Government Accountability Office, *Department of Homeland Security: Continued Progress Made Improving and Integrating Management Areas, but More Work Remains*, GAO-12-1041T, September 20, 2012, p. 6, at http://www.gao.gov/products/GAO-12-1041T.

[321] U.S. Department of Homeland Security, Chief Procurement Officer, *The Chief Procurement Officer's Four Priorities: Strategic Plan, Fiscal Year 2012 to 2014*, pp. 15-16, at http://www.dhs.gov/sites/default/files/publications/10918-02_OCPO_strategic_plan_508_2.pdf.

[322] U.S. Department of Homeland Security, "Overview of the DHS Balanced Workforce Strategy for Federal Contractors," at https://www.dhs.gov/overview-dhs-balanced-workforce-strategy-federal-contractors.

[323] Ibid.

recruit and retain the "optimal numbers" of acquisition staff it needs to conduct procurements properly? What acquisition tasks, activities, and contracts are most likely to be affected by the lack of a fully staffed and trained acquisition workforce? Under its Balanced Workforce Strategy, has DHS discovered contractor employees performing inherently governmental functions? Has the department identified any situations where it had ceded control over its mission and operations to contractor employees? How many contractors, and which contracts, might be affected by the agency's efforts to achieve a balanced workforce?

Homeland Security Research and Development

Dana A. Shea, Specialist in Science and Technology Policy (dshea@crs.loc.gov, 7-6844)

For more information, see CRS Report R43064, *The DHS S&T Directorate: Selected Issues for Congress*.

Many stakeholders have identified advances in research and development (R&D) as key to creating new or improved technologies that defend against homeland security threats. R&D is generally a multi-year endeavor with significant risk of failure. Additionally, it may take years to realize any benefits from R&D investments. The Administration and Congress have differing visions regarding successful R&D performance in DHS, as indicated by marked differences in requested and appropriated funding. In addition, some congressional and stakeholder expectations regarding the effectiveness and efficiency of agency performance have not been met. The 113th Congress may continue to focus attention on whether investments in homeland security research and development net appropriate rewards, how the distribution of investments among homeland security topics and between R&D activities leads to a balanced portfolio, and what the appropriate funding level for DHS R&D is during a time of fiscal constraint.

The DHS homeland security R&D activities have substantial scope, as these activities must attempt to meet the needs of both DHS component agencies and other customers outside of the agency, such as first responders. Many stakeholders continue to debate the optimal approach to maximizing DHS R&D effectiveness. Some advocates call for substantial increases in particular areas of research and development, citing that a dedicated research effort with significant investments is more likely to yield technology breakthroughs. Some stakeholders call for a rebalancing of the investment portfolio with an increased focus on technology development, arguing that many prototypes under development in the private sector need only a small boost to convert them to procurable technologies. Still other stakeholders call for a rebalancing of the investment portfolio towards long-term research activities, warning that DHS will lack research outcomes to develop into prototypes if long-term research languishes. Finally, portions of the stakeholder community suggest using a high-risk, high-reward investment strategy similar to that undertaken by the Defense Advanced Research Projects Agency (DARPA) so as to make "leap-ahead" advances relative to terrorist capabilities.

DHS is not the sole provider of federal funds for homeland security R&D, but the DHS Under Secretary for Science and Technology (S&T) is responsible for coordinating homeland security R&D activities within DHS and across the federal government. The DHS Under Secretary for S&T has experienced challenges in attempting to coordinate these activities and has not issued a federal homeland security R&D strategy. The GAO has identified that DHS lacks an established definition for what constitutes R&D within the agency. This may be a key barrier to coordination of R&D investment within DHS and across the broader federal effort. Congress has historically been interested in identifying and overcoming the barriers to such coordination. The 113th

Congress may conduct oversight of how any new strategic approaches taken by DHS address these long-standing concerns, set milestones for future performance, and project meeting the needs of DHS components and the first-responder community.

Both the Administration and Congress have contemplated reorganizing DHS R&D activities. For both FY2011 and FY2012, DHS requested that Congress transfer some research and development activities within the purview of the Domestic Nuclear Detection Office (DNDO) to the S&T Directorate. Congress did not approve this transfer. In contrast, the Senate explanatory statement accompanying P.L. 113-6 directed DHS to consider the advantages of merging the Office of Health Affairs and DNDO, potentially transferring portions of these offices to other DHS components. The results of the proposed merger, R&D reprioritization efforts, and consolidation might change the productivity of DHS R&D activities, which have been criticized by some stakeholders as having little to show for the federal investment. Other stakeholders, including some representatives of DHS operational components, indicate that R&D efforts undertaken by the S&T Directorate have yielded value. Congressional appropriations for the S&T Directorate have fluctuated in recent years. This may indicate that some congressional policymakers find the slow rate of return shown by S&T Directorate R&D investments unacceptable.

Author Contact Information

William L. Painter
Analyst in Emergency Management and Homeland Security Policy
wpainter@crs.loc.gov, 7-3335

John Frittelli
Specialist in Transportation Policy
jfrittelli@crs.loc.gov, 7-7033

Shawn Reese
Analyst in Emergency Management and Homeland Security Policy
sreese@crs.loc.gov, 7-0635

Bruce R. Lindsay
Analyst in American National Government
blindsay@crs.loc.gov, 7-3752

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Natalie Keegan
Analyst in American Federalism and Emergency Management Policy
nkeegan@crs.loc.gov, 7-9569

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

Lennard G. Kruger
Specialist in Science and Technology Policy
lkruger@crs.loc.gov, 7-7070

Frank Gottron
Specialist in Science and Technology Policy
fgottron@crs.loc.gov, 7-5854

Linda K. Moore
Specialist in Telecommunications Policy
lmoore@crs.loc.gov, 7-5853

Sarah A. Lister
Specialist in Public Health and Epidemiology
slister@crs.loc.gov, 7-7320

Jared T. Brown
Analyst in Emergency Management and Homeland Security Policy
jbrown@crs.loc.gov, 7-4918

R. Eric Petersen
Specialist in American National Government
epetersen@crs.loc.gov, 7-0643

L. Elaine Halchin
Specialist in American National Government
ehalchin@crs.loc.gov, 7-0646

Claudia Copeland
Specialist in Resources and Environmental Policy
ccopeland@crs.loc.gov, 7-7227

Barbara L. Schwemle
Analyst in American National Government
bschwemle@crs.loc.gov, 7-8655

Dana A. Shea
Specialist in Science and Technology Policy
dshea@crs.loc.gov, 7-6844

Henry B. Hogue
Specialist in American National Government
hhogue@crs.loc.gov, 7-0642

David Randall Peterman
Analyst in Transportation Policy
dpeterman@crs.loc.gov, 7-3267

Bart Elias
Specialist in Aviation Policy
belias@crs.loc.gov, 7-7771

Kristin Finklea
Acting Section Research Manager and Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030

Marc R. Rosenblum
Specialist in Immigration Policy
mrosenblum@crs.loc.gov, 7-7360